NEBRASKA INFORMATION TECHNOLOGY COMMISSION

Tuesday, September 30, 2003, 1:00 p.m.
Videoconference Sites:
Executive Building-Videoconference Room 103, 521 South 14th Street, Lincoln, Nebraska
Kearney Public Library-Information Center, 2nd Floor, 2020 1st Avenue, Kearney, Nebraska

AGENDA

Meeting Documents:
Click the links in the agenda or click here for all documents (1.7 MB)

1:00 p.m. Call to order and Roll Call - Lt. Governor Heineman
Notice of Meeting
Approval of **June 10, 2003 Minutes***
Public Comment

1:15 p.m. Update on Major Initiatives

A. *Telecommunications Infrastructure*
1. NETCOM/CAP - Brenda Decker
2. Statewide Telehealth Network - Anne Byers
3. Statewide Synchronous Video Network - Mike Beach
4. Interim Network Policy Work Group (Web site) - Steve Schafer

B. *Community and Economic Development*
1. Status Report on CTF and Mini-planning Grants - Anne Byers
2. Tangents (view Fall issue)
3. Toolkit Workbook (view Workbook)

C. *Delivery of Government and Educational Services*
1. Nebraska@ Online Manager Contract - Steve Schafer
2. Update on the 5th Annual E-government Conference (November 18) - Steve Schafer
3. Internet2 SEGP - Tom Rolfes

D. *Planning and Accountability*
1. Report on Security Assessment - Steve Schafer
2. **GTCF Grant Extension*** - Steve Schafer

2:30 p.m. Update on Nebraska Information System (NIS) -- Tom Conroy

3:00 p.m. Statewide Technology Plan

A. Update on Action Items

3:15 p.m. Other Reports from the Councils, Technical Panel and Staff

A. Community Council Report - (Discussed in Report on Community and Economic Development)
B. Education Council Report - Tom Rolfes
- **Membership***

C. State Government Council Report - Rick Becker
D. Technical Panel Report - Walter Weir
Recommended Standards and Guidelines*
- Wireless Local Area Network Guidelines
- Remote Access Guidelines
- Use of Computer-based Fax Services by State Government Agencies

3:45 p.m. Other Business

A. Discuss statutory restrictions on use of video conferencing for official meetings

4:00 p.m. Next Meeting Date - Thursday, November 13 , time and location to be determined.
Adjournment

(Bolded * indicate Action Items.)

Meeting notice was posted to the NITC and Public Calendar Websites on August 20, 2003.
Agenda and meeting materials were posted to the NITC website on September 24, 2003

NEBRASKA INFORMATION TECHNOLOGY COMMISSION

Tuesday, June 10, 2003,1:00 p.m. CT
Video Conference Sites:
Executive Building-Videoconference Room 103, 521 South 14th Street, Lincoln, Nebraska
Panhandle Station-High Plains Room, 4502 Avenue I, Scottsbluff, Nebraska
Kearney Public Library-Information Center, 2nd Floor, 2020 1st Avenue, Kearney, Nebraska

PROPOSED MEETING MINUTES

MEMBERS PRESENT:

Kearney Site: **Greg Adams**, Mayor, City of York; **Linda Aerni**, Chief Executive Officer, Community Internet Systems; **L. Merill Bryan**, Senior Vice President & Chief Information Officer, Union Pacific; and **Dr. Eric Brown**, Manager, KRVN Radio
Lincoln Site: **Trev Peterson**, Attorney, Knudsen, Berkheimer, Richardson, and Endacott, LLP and **Dr. L. Dennis Smith**, President, University of Nebraska
Scottsbluff Site: **Hod Kosman**, CEO, Platte Valley Financial Services

MEMBERS ABSENT: Lieutenant Governor Dave Heineman, Chair, and Dr. Doug Christensen, Commissioner, Department of Education

CALL TO ORDER, ROLL CALL, AND NOTICE OF PUBLIC MEETING

Lieutenant Governor Heineman was called to assess tornado damage caused by the previous evening's storms. In the absence of the Lieutenant Governor, Commissioner Brown chaired the meeting. The meeting was called to order at 1:35 p.m. There were seven members present at the time of roll call. A quorum existed to conduct official business. It was stated that the meeting notice was posted to the NITC and Public Calendar Websites on May 27, 2003 and that the meeting agenda and meeting materials were posted to the NITC website on June 3, 2003.

APPROVAL OF MARCH 24, 2003 MINUTES

Commissioner Adams moved to approve the March 24, 2003 minutes as presented. Commissioner Bryan seconded the motion. Roll call vote: Adams-Yes, Aerni-Yes, Brown-Yes, Bryan-Yes, Kosman-Yes, Peterson-Yes, and Smith-Yes. Results: 7-Yes, 0-No. The motion carried by unanimous vote.

PUBLIC COMMENT

Commissioner Adams introduced Matt Heller. Mr. Heller is doing an internship through the JD Edwards Program at the University of Nebraska-Lincoln. The City of York received a mini-grant from Technologies Across Nebraska's Building Information Age Communities Project. The University received funding for this project from the Nebraska Information Technology Commission Community Technology Fund.

PRESENTATION TO BRENDA DECKER

In its March 2003 issue, Government Technology Magazine recognized Brenda Decker, Director of DAS-Communications as one its "Top 25: Dreamers, Doers, and Drivers." This annual award goes to those people in the nation who have played key roles in "strengthening government operations in their jurisdictions and improving the services delivered to citizens." Commissioner Brown presented the award to Ms. Decker.<![endif]>

UPDATE ON MAJOR INITIATIVES

Telecommunications Infrastructure:

NETCOM/CAP, Brenda Decker. The Division of Communications issued an RFP on behalf of CAP (Collaborative Aggregation Partnership). Phase I will carry traffic from Omaha to Lincoln and Lincoln to Grand Island and Kearney. A team made up of University of Nebraska, Division of Communications, State College Systems and K-12 representatives evaluated four bids: Adesta, Dark Fiber Solutions, Alltel and Sprint. The Intent to Award was offered to Alltel on June 10th. Alltel will provide a MPLS (Multiple Protocol Label Switching) network. This type of network allows for use of mixed and multiple networks and different bandwidths. The management of the network would allow services that can be purchased as needed – bandwidth on demand. The cost of this network will save the state and the University of Nebraska approximately $5,000 a month. Ms. Decker entertained questions and comments.

Statewide Telehealth Network Plan, Anne Byers. The Public Service Commission approved the use of Nebraska Universal Service Fund to support telehealth. The Public Service Commission requested a plan staying under $900,000. Roger Keetle submitted the plan on May 3rd and the steering committee is currently waiting for the Public Service Commission's response. The plan will reduce line costs for hospitals to $200 per month for each T-1 circuit. Hospitals will be asked to pay $50/month for a backbone to connect regional networks. Discussions have occurred between the Telehealth Network Steering Committee and the CAP group regarding the use of the state's backbone. Ms. Byers thanked the Telehealth Subcommittee, Roger Keetle, the Nebraska Hospital Association for their commitment to this endeavor. Ms. Byers entertained questions and comments.

Statewide Synchronous Video Network, Tom Rolfes. The Technical Panel established this work group in February 2003. Members include representatives from the K-12 sector, higher education institutions, Telehealth, National Guard, Division of Communications, NETC, Department of Education, NITC, Public Service Commission, and the Omaha metro district. At the May 28, 2003 meeting, groups were formed and assigned specific tasks to accomplish the following timeline:

June 15, 2003: Revise all task group documents and post to NITC SSVWG Web site
June 15-July 30: SSVWG members communicate with and gather feedback from sub-sector peers; complete survey of distance learning networks.
July 30, 2003: All day meeting in Lincoln
August 15, 2003: Circulate first draft of preliminary recommendations
September 10, 2003: Present draft of recommendations to NITC Technical Panel
Late September: All day meeting, Location TBA

Mr. Rolfes entertained questions and comments.

Community and Economic Development
Technology Across Nebraska Survey Results, Anne Byers. Surveys were sent to 25 applicants for the Community IT Planning and Mini Grant program. Sixteen surveys were returned, yielding a response rate of 64%. The survey results should not be interpreted as representative of all communities in Nebraska. Some of the survey results were reviewed. Recommendations from the survey were as follows:

1. Publish an e-mail newsletter on technology-related development.
2. Continue to maintain and update the TAN and Community IT Toolkit Web sites.
3. Add funding information to the Community IT Toolkit Web site.
4. Work with TAN partners to develop and deliver regional workshops on IT-related economic development.
5. Continue the IT Planning and Mini Grant program.

Status Report on Mini-planning Grants, Anne Byers. Eighteen communities were to submit their IT plans by June 1st but are taking longer. Two communities have hired interns to assist with their IT planning – York and Broken Bow. The workbook has been helpful to communities and it will be revised this summer. Currently, applications are being accepted for the second round of funding for the mini-grants. Applications are due on July 1.

Delivery of Government and Educational Services

E-government Strategy, Rick Becker, Government Information Technology Manager. A number of enhancements on the State of Nebraska's web site will be made over the next few months. Progress is being made in regards to forms automation. Nebrask@Online has developed an online payment process and several interactive licenses. Nebrask@Online's contract with the state is expiring. The Records Board has issued an RFP for the maintenance of State of Nebraska web site. Bids are due on July 31st with a contract award in September.

Annual E-Government Conference, Steve Schafer, Chief Information Officer. The next E-government Conference is scheduled for November 18th. Government Technology Magazine is a partner and co-sponsor. The League of Municipalities and NACO will be invited to attend. The format will be different. There will be several on-going concurrent sessions of different topics.

E-Learning Initiative, Dr. Jean Jones and Jim Zemke. Dr. Jones was not available for today's meeting. Mr. Zemke provided background information on the Statewide eLearning Initiative, as well as activities occurring in the higher education and K-12 sectors. Future activities include:

- Define eLearning goals and objectives
- Identify Initiative "sponsor" (candidates = NITC, P-16, Nebraska Department of Education, NCITE, others)
- Organize NE eLearning Consortium – address that issues of structure, membership, governance, accountability, authority, etc.

Planning and Accountability

Security Initiatives, Steve Schafer, Chief Information Officer. Commissioners were provided a written report prior to the meeting. Mr. Schafer did not review the document but offered to answer any questions and/or provide clarification.

STATEWIDE TECHNOLOGY PLAN
Steve Schafer, Chief Information Officer

There were some changes made in the organization and content of the plan. A new section serves as an introduction and explains the purpose and scope of the plan. The purpose of the Statewide Technology Plan is to set forth the vision and goals for the use of information technology in Nebraska, with a set of action items that will guide the work of the NITC and its councils. The Statewide Technology Plan does not allocate funding among technology projects. Section 2 reflects the mission and goals of the NITC. Council priorities are now included in this section. They represent specific objectives for accomplishing the four NITC goals. Section 3 is the Action Plan. It follows the same format as previous years, except that action items are organized around the four goals of the NITC, rather than being listed by the sponsoring Council. Section 4 provides effectiveness measures, including a summary of progress on last year's action items. Content is also organized by the NITC goals.

Commissioner Aerni moved to approve the update of the 2003-2004 Statewide Technology Plan. Commissioner Adams seconded the motion. Roll call vote: Bryan-Yes, Kosman-Yes, Brown-Yes, Peterson-Yes, Aerni-Yes, Smith-Yes, and Adam-Yes. Results: 7-Yes, 0-No. The motion carried.

OTHER REPORTS FROM THE COUNCILS, TECHNICAL PANEL AND STAFF

COMMUNITY COUNCIL, Anne Byers, Community Information Technology Manager

The Community Council met in May to adopt action items included in the Statewide Technology Plan. Other business was previously reported.

EDUCATION COUNCIL, Tom Rolfes, Education Information Technology Manager

At the May meeting, the council had two action items – Recommendation to the NITC for 2003-2004 Action Items and Membership Recommendations. An Internet2 presentation co-sponsored by the University of Nebraska-Lincoln and the Education Council followed the May 16th business meeting.

The Education Council unanimously voted to forward the following membership recommendations to the NITC for final approval:

- Higher Education Renewals: Jack Huck (Community College System), alt. Bill Path and Tom Krepel (State College System) alt. Robin Smith

- Higher Education New Members: Chuck Lenosky (Independent Colleges and Universities-Replacing Dietz) alt. Jerry Harnisch and Rob Manzer (Independent Colleges and Universities-Pro tem O'Neill) alt. Thomas O'Neill, Jr.
- K-12 Education Renewals: Linda Engel (Public School Teachers) alt. Renee Bose; Joe LeDuc (Private/Parochial School Teachers) alt. Tom Korta; Ed Rastovski (School Administrators) alt. Keith Rohwer; and Al Schneider (Educational Service Units) alt. Wayne Bell
- K-12 Education New Member: Michael Pate (Boards of Education-Pro tem Bartels) alt. Linda Richards

Commissioner Kosman moved to approve the Education Council's membership recommendations. Commissioner Byran seconded the motion. Roll call vote: Brown-Yes, Peterson-Yes, Aerni-Yes, Smith-Yes, Adam-Yes, Kosman-Yes, and Bryan-Yes. Results: 7-Yes, 0-No. The motion carried.

STATE GOVERNMENT COUNCIL, Steve Schafer. The council has met once since the last NITC meeting. The State Government Council updated the action items and also discussed technical standards/guidelines recommendations for state government.

TECHNICAL PANEL REPORT, Walter Weir, Chair. The Technical Panel has met twice since last the NITC meeting. In April, the panel traveled to Kearney to tour the University Nebraska-Kearney and Good Samaritan Hospital. Mr. Weir complimented Ms. Decker, as well as Sid McCartney, on their work and efforts with NETCOM. The Technical Panel will be assisting with the development of a business plan for the new state network.

STAFF REPORT

E-government Survey Options, Rick Becker, Government Information Technology Manager. One option is to have staff work with Nebrask@Online to develop a web-based survey. Another option would be to contract for a scientific survey at a cost of approximately $20,000. Another option is to utilize national reports that have already been done. After discussion of the options, Mr. Schafer was directed to pursue the web-based survey.

Update on E-mail Systems, Rick Becker, Government Information Technology Manager. At their meeting on May 8th, the State Government Council identified 12 topics for further review as possible technical standards, guidelines or enterprise solutions. Revising the Electronic Mail Standard is one of the topics the Council is considering. Interest stems from the phasing out of the OfficeVision product; interest in greater efficiency and economy; and security related issues.

I.T. Expenditures, Steve Schafer, Chief Information Officer. Staff has been researching several different resources and is pulling the data for a report. Agencies have submitted IT plans but have found out that some of them did not include any information on IT spending. It is anticipated to have a report for the September meeting. Another source of information will be the new NIS accounting system but there are details of this particular feature that need to be worked on before it's implementation.

Commissioners would like an update on the NIS Project and implementation for the next meeting. Commissioner Bryan was thanked for the panel presentation conducted at the March meeting.

OTHER BUSINESS

There was no other business.

NEXT MEETING DATE

The next meeting of the Nebraska Information Technology Commission will be held on September 30th, 1:00 p.m. CT, location to be determined.

With no further business, Commissioner Adams moved to adjourn. Commissioner Bryan seconded the motion. All were in favor. The motion carried by voice vote.

The meeting was adjourned at 3:08 p.m.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by the staff of the Office of the CIO/NITC.

Nebraska Telehealth Network Update

September 23, 2003

Background. On December 17, the Public Service Commission issued an order authorizing the support of telehealth from the Nebraska Universal Service Fund. The order directed the Nebraska Hospital Association to submit a plan which would define how the Nebraska Universal Service Fund support should be used to support rural health care providers. The Nebraska Hospital Association, with support from the NITC, developed and submitted a plan to the Public Service Commission in late May. The plan provided a starting point for discussions with the Public Service Commission.

Recent Developments. On September 17, representatives of the regional medical centers which will serve as hubs for the telehealth network, the Public Service Commission, the Nebraska Hospital Association, and the Nebraska Information Technology Commission met. The meeting addressed several concerns expressed by the Public Service Commission.

Representatives of the hub hospitals agreed to the following:

- Hub hospitals agree to use the communication standards, protocols and equipment that comply with or are interoperable with the standards established by the Nebraska Information Technology Commission.
- Hub hospitals certify that they have entered into an agreement with an agent designated by the Nebraska Public Service Commission to provide data to evaluate the performance of the Nebraska Telehealth Plan.
- The design of the telehealth system of the hub hospitals shall not eliminate the participation of any hospital or system because of proprietary equipment, operations systems or membership in associations or affiliation with a particular medical or technical organization.
- Hub hospitals have entered into an agreement or agreements to support hospitals licensed as Critical Access Hospitals or to provide clinical telehealth services, telehealth educational programs or teleradiology services.
- Hub hospitals have entered into an agreement to allow any hospital on the network to connect to another hospital.

Efforts are also being made to incorporate bioterrorism preparedness into the plan for the Nebraska Telehealth Network. The Nebraska Hospital Association has received financial support for further development of plans for the Nebraska Telehealth Network.

NITC Technical Panel
Statewide Synchronous Video Work Group

Update and Round One Recommendations
September 17, 2003
Michael Beach, Sponsor

Preliminary Round One Recommendations:

1. Recommend a State-level Internet Protocol (IP) network that maintains a satisfactory, user-defined Quality of Service for interactive distance learning, telemedicine, videoconferencing and data.
2. Recommend two contracts at the local level; one for procurement and maintenance of connective terminal hardware and another one for transport. One contract may be considered as long as the end-user has full access to and flexible use of all bandwidth on the network and has the ability to upgrade video equipment as desired.
3. If the authority does not already exist, recommend to the NITC that it work with the Public Service Commission to draft clarification language that allows providers to offer different service rates for public and private entities.
4. If the authority does not already exist, recommend to the NITC that it work with the Legislature to authorize a discounted rate for public entities for data services within flexibly provisioned bandwidth.
5. Recommend to the NITC that it work with the Legislature and the Public Service Commission to provide a one-time capital investment, compliant with NITC technical standards, for the replacement or upgrade of equipment at existing sites when current contracts expire or are re-negotiated.

Next Steps:

- Distribute first five recommendations to the SSVWG and ask for feedback and modifications by August 6, 2003 (Tom Rolfes).
- Present draft Round One recommendations to the NITC Technical Panel on August 13, 2003 (Mike Beach).
- Research current authority for recommendations #3 and #4 (Gene Hand).
- Begin cost estimations for recommendation #5 (John Horvath, Jeff McCartney)
- Complete survey on each distance learning network by September 30 (SSVWG members)
- Provide briefing to the Public Service Commission on the Statewide Synchronous Video Work Group on August 26, 2003 (Mike Beach, Gene Hand, Brenda Decker).
- Begin discussions with the telecommunication providers about an IP-centric network and flexibly provisioned bandwidth before the end of August 2003 (Steve Schafer, Mike Beach, Brenda Decker, Rick Golden, Gene Hand).
- Present final Round One recommendations to the NITC Technical Panel on September 17, 2003 (Mike Beach)
- Ask for approval of the Round One recommendations by the NITC on September 30, 2003 (Walter Weir).

The next meeting date and location of this work group has not been determined but it will be in early October. Previous Meetings: March 26, May 28, July 30, 2003.

September 16, 2003

Michael Beach, Chair
Nebraska Educational Telecommunications
P.O. Box 83111
Lincoln, NE 68501

Dear Mr. Beach:

The Commission is impressed with the progress reported by the Statewide Synchronous Video Network Work Group (SSVNWG) at our public meeting held August 26, 2003, to address the future of distance learning in Nebraska. We opened Docket No. C-2874/PI-71 in February of this year in response to concerns relative to distance learning and on March 18, 2003, a workshop was held at the Commission by videoconference with links to Columbus, Grand Island, Hastings, Kearney, McCook, North Platte, Norfolk, O'Neill, and Scottsbluff. Several parties provided information addressing several distance learning issues, and after the workshop concluded, it was clear that further technical collaboration was necessary to develop a comprehensive plan for the future. We believe the efforts of the SSVNWG have been significant and a plan for the future is beginning to take shape.

There were two issues identified during the SSVNWG report on which the group sought guidance from the Commission. The two issues were: 1) how the future service would be tariffed, and 2) what options were available to fund the conversion to an Internet Protocol (IP) centric network.

Regarding the first issue, there appear to be several options at this time with respect to how the network would be structured including what equipment would be provided by the carriers. We believe there actually may be options for the schools, based on their ability to pay for equipment up front, that would result in several different service offerings and the resulting tariffs. A thorough analysis that considers the available support from the School and Library Division (SLD) of the Universal Service Administrative Company (USAC) should be conducted for both the equipment and transport necessary to support the network prior to selecting the appropriate service from the selected carrier. Tariff issues relative to distance learning can be resolved once the parameters for the service are defined.

The second issue is how to fund, over a 3-5 year period, the conversion to an IP network estimated to cost $10 million above the current rates charged to the participating schools. There were suggestions that the Nebraska Universal Service Fund (NUSF) provide support for deploying this new education network. The Commission is currently conducting significant reform of the support to high cost rural areas. At the same time, we are committed to implementing a telehealth network with annual support from the fund. The uncertainty of the future demands on the fund for these supported services prevents us from considering further commitments at this time.

We understand the importance of moving forward and addressing the associated funding requirement. Therefore, we recommend that a work group be assembled to address the funding issue. Once the Nebraska Information Technology Commission (NITC) has formally adopted the SSVNWG recommendations, the work group should be prepared to investigate funding sources such as RUS grants, federal USF support from the SLD, philanthropic foundations and/or state funding provided by the legislature.

We remain concerned about the future of distance learning in Nebraska and are encouraged by your report, which recommends a state-level IP network be developed. As such, we stand ready and willing to participate on the funding work group.

Sincerely,

Anne C. Boyle, Chair

Gerald L. Vap, Vice-Chair

Lowell C. Johnson

Rod Johnson

Frank E. Landis

cc: Brenda Decker, DOC
Tom Rolfes, NITC
Wayne Fisher, DOE

September 23, 2003

To: NITC Commissioners

From: Anne Byers, Community IT Manager

Subject: Activities Addressing Community and Economic Development

I will not be able to attend the NITC meeting on Sept. 30. However, I have prepared a number of documents giving an update on Community Council activities which address community and economic development. If you have any questions or would like additional information, please e-mail abyers@notes.state.ne.us.

Community Technology Fund Report. Projects funded through the 2002 Community Technology Fund range from the development of a municipal wireless network used to improve the delivery of local government services to the placement of computers in local learning centers to expand access to educational opportunities in rural areas. More information on these projects can be found in the meeting materials.

IT Planning and Mini Grant Program. In the fall of 2002, eight communities and regional groups began conducting technology assessments and developing a technology plan using the *IT Planning and Assessment Workbook*. Each participating community received a $2,500 mini grant to support their IT planning efforts. As of Sept. 22, 2003, six of the eight communities and regional groups have completed technology plans. Alliance, Custer County, Edgar, Keya Paha/Brown/Rock Counties, West Point and York have prepared technology plans and are moving into the implementation phase. The remaining two committees are also making progress. The Crawford-Harrison technology committee has applied for a grant from the USDA Rural Utilities Service and is waiting to hear if their application has been funded before developing a formal technology plan. The Fillmore County technology committee expects to have their plan completed by the end of October. Additional information on the progress of each of the participating technology committees can be found in the meeting materials.

Six more community and regional groups are participating in the 2003-2004 IT Planning and Mini Grant Program. Ord, Homer, and Hastings have already held their initial committee meetings. Other participating communities include Dakota City, Maskell, and Lexington.

TANgents. In the spring, Technologies Across Nebraska surveyed community technology committees to determine their training needs and preferred methods of receiving training. The most preferred method of receiving information was through an electronic newsletter. Accordingly, Technologies Across Nebraska has begun publishing TANgents, a quarterly electronic newsletter. The newsletter provides an opportunity to involve Technologies Across Nebraska partners. Contributors to the first issue include Gene Hand, Public Service Commission; Roger Keetle, Nebraska Hospital Association; Steve Williams; Department of Economic Development; Jim Emal, University of

Nebraska; Glen Cox, University of Nebraska Rural Initiative; Phyllis Schoenholz, University of Nebraska Extension; and Lance Martin, City of South Sioux City. TANgents currently reaches approximately 1,500 individuals. If you would like to be added to the TANgents mailing list, please e-mail me at abyers@notes.state.ne.us or let Steve Schafer know at the meeting.

Community IT Planning Workbook. The workbook is beginning to gain national recognition as a valuable resource. The NITC has already received a request from Minnesota to use the workbook in a broadband promotion project. After being pilot tested by participants in the first year of the IT Planning and Mini Grant program, the workbook was revised and expanded. Participants suggested that sample plans and a glossary of technology terms be included. These changes were made to the revised *Community IT Planning Workbook*. In addition, the facilitator's guide was revised and includes tips gleaned from working with the participating communities as well as tips from community leaders. Additional worksheets to help committees plan supplemental assessment activities, build community support, develop a technology plan, and plan implementation activities were also developed. The Community IT Planning Workbook is available at www.nitc.state.ne.us/toolkit/workbook.

Nebraska Information Technology Commission

Community Technology Fund Projects 2002

With the development of a municipal wireless network with funding from the NITC's Community Technolgy Fund, the South Sioux City Police Department became the first law enforcement agency in the state to access the Nebraska Criminal Justice Information System's Web interface from the patrol care.

Grants support technology development

Since September 1998, 40 projects have been awarded a total of $834,700 from the Nebraska Information Technology Commission's Community Technology Fund. The projects funded demonstrate how information technology is being used to improve efficiency and enhance economic development. Projects funded through the 2002 Community Technology Fund range from the development of a municipal wireless network used to improve the delivery of local government services to the placement of computers in local learning centers to expand access to educational opportunities in rural areas. This report highlights the projects funded from the 2002 round of the Community Technology Fund and shares lessons that can be learned from these projects.

2002 Community Technology Fund Projects

Project: Wireless Municipal Area Network

Entity: City of South Sioux City

Award: $13,250

Status: Complete

The City of South Sioux City has installed ten high-speed wireless "hotspots" in the community for use by the police department, fire department, public library and South Sioux City Community Schools. The South Sioux City Police Department became the first law enforcement agency in the state to access the Nebraska Criminal Justice Information System's Web interface from the patrol car. Through a partnership with the South Sioux City Community Schools, the police are able to view 48 different video surveillance cameras in the Senior High School complex from the patrol car in real time. The South Sioux City School District is utilizing the wireless network to provide connectivity for school board meetings, field research for science class, and real-time updates and weather reports for sporting events. The South Sioux City Fire Department is utilizing the wireless network to gain access to Internet and e-mail at the fire hall. The Fire Department is also using the system to gain access to training resources and to access real-time information on HAZMAT as well. The South Sioux City Public Library is using their wireless access point to provide library patrons an alternative for public access computing. Patrons can utilize wireless-enabled laptops to access the Internet or do homework from the location they feel most comfortable. The South Sioux City Housing Authority is utilizing the wireless network to improve their access to Internet and e-mail.

Lessons Learned:

Much has been learned about the deployment, maintenance, and security of a wireless network. Omni directional antennas were utilized in the early testing and deployment of the network until it was discovered that two antennas installed in a diversity configuration was a far superior set-up. Signal quality and range is greatly enhanced by utilizing the multi-path canceling abilities of a diversity antenna configuration. A service pack upgrade is available for Microsoft Internet Explorer version 6 that enables the 128 bit cipher strength required for law enforcement to access NCJIS. Most of the connectivity done on the wireless also utilizes VPN. Several enhancements to 802.11 security are embedded in the newly released Microsoft Windows Server 2003. The City of South Sioux City plans to implement Server 2003 on all of its servers this fall.

Some of the greatest challenges of the project turned out not to be technical or physical challenges—but more political and policy challenges. Acceptable use policies had to be developed for the library and police department as well as policies for patrons to use library laptops. An agreement had to be reached for the Housing Authority to access the network as well. Often times, the development of policies and agreements is far more complex and time-consuming than the actual installation of the equipment.

Project: Building Information Age Communities Planning Mini Grants

Entity: University of Nebraska Cooperative Extension

Award: $20,000

Status: Extended until October 31, 2003

In the fall of 2002, eight communities and regional groups began conducting technology assessments and developing a technology plan using the *IT Planning and Assessment Workbook*. As of Sept. 22, 2003, six of the eight communities and regional groups have completed technology plans. Alliance, Custer County, Edgar, Keya Paha/Brown/Rock Counties, West Point and York have prepared technology plans. The remaining two committees are making progress. The Crawford-Harrison technology committee has applied for a grant from the USDA Rural Utilities Service and is waiting to hear if their application has been funded before developing a formal technology plan. The Fillmore County technology committee expects to have their plan completed by the end of October.

Lessons Learned:

1. Community technology planning requires a substantial time commitment from technology committee members and facilitation by energetic, committed community leaders. The mini grant program provided an incentive for communities to focus on technology planning.

2. The *Community IT Planning Workbook* simplifies the planning process. Participants liked the workbook and appreciated not having to develop their own assessment and planning tools. Participants suggested that sample plans and a glossary of technology terms be included. These changes were made to the revised *Community IT Planning Workbook*. In addition, the facilitator’s guide was revised and includes tips gleaned from working with the participating communities as well as tips from community leaders. Additional worksheets to help committees plan supplemental assessment activities, build community support, develop a technology plan, and plan implementation activities were also developed.

3. Sometimes forming a technology committee can attract the attention of telecommunications providers, facilitating discussions between the community and providers on the availability and deployment of advanced services.

4. Documenting community needs through the assessment process can assist in the preparation of successful grant applications.

Future Plans

Six more community and regional groups are participating in the 2003-2004 IT Planning and Mini Grant Program. Ord, Homer, and Hastings have already held their initial committee meetings. Other participating communities include Dakota City, Maskell, and Lexington.

Project: Digital City Hall

Entity: City of Ashland

Award: $7,629

Status: Complete

The City of Ashland purchased a LaserFiche system to scan city documents into a format that is easily searchable, provides more convenient access to the public and staff, and allows for secure, off-site storage of city records. Many members of the community are eager for the documents to be in a digital format and be accessible via the city's Web site.

Lessons Learned: Through the project, staff has learned the importance of technology and how critical digital preservation is. It would be beneficial to have a staff member and computer dedicated to this project.

Project: City of Aurora Utilities GIS

Entity: City of Aurora

Award: $25,000

Status: Complete

The City of Aurora designed and created a utilities database that captures all the necessary information items desired by city administrators and staff. By using GIS resources currently available from other governmental jurisdictions, the City of Aurora has demonstrated that GIS can be an affordable and useful tool for smaller communities in Nebraska. The City of Aurora has entered into an agreement with Hamilton County to share software that both agencies require. This has already generated an immediate $3,000 in savings. In addition, the City of Aurora has exchanged utilities information with NPPD in exchange for new 2002 imagery flown by NPPD, saving the city the expense of duplicating the imagery and saving NPPD the expense of creating the utility data it requires.

Initial benefits of this project include the general overhaul of the utilities system. The creation of the GIS and records management system has forced the city field crews to locate all services in the field (for example, buried valves and manholes). It is also forced field crews to perform preventative maintenance on items that may not have been considered, leading to more expensive repairs and/or utility outages at a later date.

Lessons Learned:

Communities undertaking a similar project should begin contacting engineering companies holding digital data early. Creating and signing agreements with these companies takes time. GPS data collection was much more rapid when crews went out beforehand to locate features with spray paint, allowing GPS collection crews to move rapidly through the city.

Project: Electronic Archiving of Medical Records

Entity: Franklin County Memorial Hospital

Award: $22,292

Status: Complete

Franklin County Memorial Hospital has implemented an electronic medical records system. The hospital has scanned 150 medical records from paper to electronic storage, created batch indexes and created a database that is accessible by password security, for reference. The PaperStore software has allowed the hospital business office to convert month-end financial reports to electronic storage, accessed through the hospital's Dairyland Software for fiscal reporting. Primary beneficiaries are the patients and providers. Having access to current information on patients will improve patient outcomes. A secondary benefit is improved compliance with HIPAA as privacy and security are improved with a password and firewall protected software.

Lessons Learned:

Ample time for scanning should be allotted. Future projects should carefully evaluate the time required to collate charts and create the patient index. Other hospitals undertaking a similar project should budget for one to two full-time equivalent staff members to scan the documents. Scanning requires staff who are detail-oriented and have both computer and organizational skills.

Project: Sarpy County GIS Base Map Interlocal Agreement

Entity: Sarpy County

Award: $25,000

Status: Complete

The Sarpy County Geographical Information System Coalition was created to develop a unified GIS in Sarpy County. This grant has partially funded the development of a GIS land base map through a contract with an engineering firm with assistance from a software/technical consultant. The development of a single county-wide land base map will allow each entity to overlay specific information without having to duplicate the efforts required to create and maintain basic information regarding the location and description of streets, lots, rivers, section lines, etc. The development of the GIS will greatly enhance the accessibility of information to local government departments, decision-makers, and to the public. As an example of the initial uses of the system and the preliminary data available, the Assessors office has been able to provide the public better information during the assessment process by utilizing the aerial photos and legal lots in conjunction with the state soils information. This project has also improved communication between Sarpy County and its cities. This has improved many processes and workflows between the participating entities.

Lessons Learned:

The main thing learned from this project is the critical role all participating members must play. A project of this size and with seven jurisdictions involved requires a huge amount of communication and organization. It is important to solidify the partnerships needed to accomplish your project. Hiring a GIS Coordinator at an earlier stage would have made the project run a lot smoother and taken some of the burden off of staff.

Project: Sink or Swim—Educating the Rural Labor Pool

Entity: Central Community College

Award: $18, 518

Status: Complete

Central Community College placed computer work stations and printers in 9 learning centers located in South Central Nebraska. Training sessions were held for learning center managers. Between mid-January and mid-May 2003, approximately 500 people have used the computers for a total of 282 hours at the ten sites. Nearly 60 percent of the users were Central Community College students completing course assignments. Enrollment in Central Community College credit courses from Spring 2002 to Spring 2003 at the nine learning center sites increased 52%.

Lessons Learned:

One of the unexpected outcomes from this project has been the realization that a large number of persons in these nine communities (Alma, Axtell, Blue Hill, Franklin, Harvard, Hildreth, Lawrence, Nelson, Orleans, and Superior) have very limited access to computer technology. Many adults have expressed an appreciation of the availability of additional computers for public use. As a result, an interest in pursuing computer-related training has increased.

Project: Basic Scanning Classes

Entity: LaVista Public Library

Award: $3,612.06

Status: Complete

Basic scanning classes are now offered at the LaVista Public Library to the public and staff of the City of LaVista, LaVista Public Library, and Metropolitan Community College.

Lessons Learned:

The project reinforced the fact that teamwork is essential. People are always willing to go the extra mile.

Project: Interactive Video/Distance Learning Network

Entity: Valley County Hospital

Award: $19,623

Status: Six-month extension granted

The development of a statewide telehealth network has delayed implementation of this project. As plans for the statewide telehealth are developed, Valley County Hospital will be better able to determine how to proceed with this project.

Project: Interactive Video/Distance Learning Network

Entity: Cherry County Hospital

Award: $11,136

Status: Six-month extension granted

The development of a statewide telehealth network has delayed implementation of this project. As plans for the statewide telehealth are developed, Cherry County Hospital will be better able to determine how to proceed with this project.

Project: Connect IT Omaha

Entity: Omaha Public Library

Award: $25,000

Status: Terminated by mutual agreement

The grantee opted not to implement this project.

Community Technology Fund Grants

1998-2002

Year	Recipient	Project	Award
2002	City of Ashland	Ashland Digital City Hall	$7,629
2002	Sarpy County	GIS Base Map Interlocal Agreement	$25,000
2002	LaVista Public Library	Basic Scanning Classes	$3,612.06
2002	Cherry County Hospital	Interactive Video/Distance Learning Network	$11,136
2002	Valley County Hospital	Interactive Video/Distance Learning Network	$19,623
2002	Omaha Public Library	Connect IT Omaha	$25,000
2002	City of Aurora	Utilities GIS	$25,000
2002	Central Community College	Sink or Swim--Educating the Rural Labor Pool	$18,518
2002	University of Nebraska Cooperative Extension	Building Information Age Communities Planning Mini Grants	$20,000
2002	Franklin County Memorial Hospital	Electronic Archiving of Medical Records	$22,292
2002	City of South Sioux City	Wireless Municipal Area Network	$13,250
2001	City of Aurora	Aurora Technology Center	$25,000
2001	Lower Platte North NRD	Common Framework for Integrating Surface Water Data	$24,800
2001	Bruun Memorial Public Library, Humboldt PublicSchool Library Table Rock-Steinauer School Library	Taking Resources and Information Online (TRIO)	$18,600
2001	Southeast Community College	Technology-Based Education for Health Occupations	$18,195
2001	Beatrice Public Library	Senior Connection	$22,932
2001	Commission for the Deaf & Hard of Hearing	Telehealth	$25,000
2001	Omaha Tribe of Nebraska	Omaha Tribe Online Information Technology Plan	$25,000
2001	Village of Brainard	Brainard Community Technology Center	$18,495
2001	Kimball County Hospital Clinic	Integrated Practice Mgmt & Electronic Medical Record Proj.	$25,000
2001	Village of Greeley	Greeley Learning and Technology Center	$23,500
2001	City of Lincoln	City of Lincoln Technology Infrastructure Audit	$23,500
2001	Central Community College	From Plowshares to PCs: Creating a Learning Community	$23,500
2000	Norfolk Public Library Columbus Public Library Northeast Nebraska Community College Library	ONE Library	$25,000
2000	Kearney Public Library	Public Internet Access Enhancement	$19,380
2000	Public Library System, Holdrege	Public Library System Web Catalog	$9,218
2000	University of Nebraska Cooperative Extension Center for Rural Community Revitalization AIM Institute	Connecting Nebraska E-Business Project	$52,000
2000	Elmwood-Murdock Public Schools	Web Parent Teacher Project	$22,270
1999	University of Nebraska	Nebraska Electronic Main Street Program	$9,990
1999	City of Wayne	NRICHN (NE Nebraska Regional Information Clearinghouse)	$2,000
1998	Dakota City Public Library	Dakota City Teleliteracy: Train the Trainers	$3,600
1998	City of South Sioux City	South Sioux City E-Commerce Initiative	8,340
1998	City of Lincoln/Lancaster County	Project Interlinc	$23,520
1998	University of Nebraska	Roving Computer Lab and Training for NE Nebraska	$28,000
1998	Lincoln Area Agency on Aging	GOAL Computer Center	$4,000
1998	Partnership for Rural Nebraska	Nebraska Teleliteracy and Electronic Commerce Initiative	$85,000
1998	Chase County	Chase County Video Development	$8,095
1998	Southeast Nebraska Development District	Teletraining for Emergency Responders	$22,000
1998	Panhandle Area Development District	Capacity Building, Communication & Cooperation	$6,225
1998	City of Superior	Business Incubator/Technology Project	$41,480
	TOTAL		**$834,700**

Building Information Age Communities

IT Planning and Mini Grant Program

Progress Report

September 23, 2003

A Cooperative Effort of
University of Nebraska Cooperative Extension
Technologies Across Nebraska
and the Nebraska Information Technology Commission

IT Planning and Mini Grant Program

In the fall of 2002, eight communities and regional groups began conducting technology assessments and developing a technology plan using the *IT Planning and Assessment Workbook*. Each participating community received a $2,500 mini grant to support their IT planning efforts. As of Sept. 22, 2003, six of the eight communities and regional groups have completed technology plans. Alliance, Custer County, Edgar, Keya Paha/Brown/Rock Counties, West Point and York have prepared technology plans and are moving into the implementation phase. The remaining two committees are also making progress. The Crawford-Harrison technology committee has applied for a grant from the USDA Rural Utilities Service and is waiting to hear if their application has been funded before developing a formal technology plan. The Fillmore County technology committee expects to have their plan completed by the end of October.

Alliance

The Box Butte County Information Technology Committee surveyed local businesses to determine their technology training needs. The survey revealed that many businesses needed basic computer training. Using information from the survey and their initial assessment, the committee developed a technology plan, identifying education, promoting e-commerce, and infrastructure development as priority areas. The technology committee has already begun implementing their plan, focusing on providing one-on-one training for area businesses and offering classes. Through a cooperative effort with REAP, an e-commerce class will start in mid-October. The IT Committee will be offering partial scholarships for participants. The committee has also compiled a list of online training opportunities. The Box Butte County Information Technology Committee's planned action steps for addressing the technology training needs of businesses and residents are included below:

Planned Action Steps

1. Organize New Classes

   Information gathered from our survey pointed out the need for beginner level classes on many subjects. These will be offered on a flexible time schedule to fit into varied work schedules.

2. Advertise and Promote Current and New Class Offerings

   We will build public awareness of educational opportunities through a variety of advertising media.

3. Develop Mentoring Activities and Support

   We will work to organize a pool of IT professionals to act as mentors for businesses and individuals. Our new laptop will allow these individuals to take education and assistance directly to consumers to help them better understand the technology and its applications.

4. Find Innovative Approaches to Best Utilize Limited IT Resources

   Computer labs needed for training are limited in number and often unavailable. The Committee will research ways to use these resources during off-hours, as well as attempt to locate additional equipment and training sites.

5. Research Use of Cable TV Channel as a Delivery Method for Free Community Education

   The local cable television company has a local community access channel available for public use. The Committee will work to develop a series of free classes to be broadcast on this channel.

Custer County

In Custer County, several priorities and action items were identified by the community, including:

- Addressing the need for DSL in the community;
- Redesigning the Broken Bow Chamber of Commerce Web site;
- Redesigning the Custer County Web site; and
- Working with local businesses to address their technology needs.

Mike Wrenholt, a student at the University of Nebraska, spent the summer in Broken Bow working on these activities as an intern through the J.D. Edwards Honor Program, The University of Nebraska Rural Initiative and Congressman Osborne's office.

Wrenholt did background research on deploying DSL in Broken Bow and helped organize a meeting with the president of Qwest Nebraska, Rex Fisher. Due to the large interest shown at that meeting, Broken Bow has moved up on Qwest's list of cities to receive DSL. Wrenholt also updated the Web sites for the Chamber of Commerce and Custer County. Several local businesses also received assistance from Wrenholt.

Crawford-Harrison

Crawford identified broadband access as their highest priority. Although smaller, Harrison has broadband access through the local cable company. Crawford and Harrison conducted a community survey to better determine community usage of the Internet. Crawford also conducted an engineering study. The information from the survey and the engineering study was used to prepare an application for the Rural Utilities Service Community Connect Broadband Grant Program. At last report, Crawford's application is still being considered for a second round of awards. Further development of the technology plan is on hold until the community is informed of the results of the Community Connect grant competition. If Crawford does not receive a grant, the community is considering proceeding without the grant.

Crawford is also developing a city Web site (www.crawfornebraska.net) It is being developed as a community bulletin board and community center as well. A priority at this time is to get city information and services online.The next phase is to help local businesses develop Web sites. Future plans include being able to develop and offer Web-based courses.

Edgar

At their initial meeting, the technology committee in Edgar narrowed down the assessment areas in the *Building Information Age Communities E-readiness Assessment* to four areas: community leadership and support; telecommunications infrastructure; technology literacy and access; and economic development and e-commerce. The Edgar technology committee worked with Kay Payne at the Center for Rural Research and Development at the University of Nebraska--Kearney to conduct a community survey which included a section on information technology. The surveys were hand-delivered and picked up by community volunteers, leading to a very high response rate (87%). The survey indicated that there was strong community support for a community center and a high level of interest in participating in computer training.

The survey found:

- In only 30% of the households, could no one operate a computer.
- Sixty-two percent of households owned a computer.

- Forty-nine percent of households have Internet access at home.
- Seventy-seven percent of home-based businesses have Internet access.
- Sixty-five percent of businesses owned by Edgar residents (both within the city limits and in the surrounding rural area) have Internet access.
- Fifty-two percent of households are interested in computer education. The total number of individuals interested in attending computer training is estimated at nearly 200.
- Edgar is relatively youthful. Forty-four percent of households have children in K-12. Those 35-44 years old (20%) and 45-54 years old (18%) comprised the largest population segments.

In July, Edgar received a $250,000 Community Development Block Grant to build a community center. In September, Edgar completed their technology plan. The community center is a key component of the plan. Plans for the new Edgar Community Center will incorporate spaces for a multimedia center and an Information Technology Learning Center, including teleconferencing capability. Other action items include expanding the upcoming Department of Economic Development Business Retention and Expansion Survey to include a survey of all major businesses in Edgar as to their current usage, capabilities and needs for e-commerce, e-marketing, and training. Training will be offered to meet the needs identified in the business survey. The revitalization of the community Web site is also planned.

Fillmore County

The Fillmore County technology committee conducted a community survey and is currently finishing their assessment and technology plan. The survey found that 75% of the households responding had a computer. Approximately two-thirds of the households had Internet access, with approximately 14% of the households having broadband access. There was considerable interest in computer training opportunities. Over 40% of the households indicated an interest in participating in local computer training classes.

Businesses also showed a high rate of computer use. Nearly all businesses (97%) reported having a computer, and 86% of the businesses had Internet access. Approximately 30% of the businesses had broadband Internet access. Employees in over 50% of the businesses have e-mail accounts. Approximately 30% of the businesses have Web sites; 5% of the businesses have full-service e-commerce sites capable of taking orders. Businesses are using computers for accounting (76%), research (72%), payroll (46%), and inventory (43%). Businesses report a strong interest in computer training. Approximately 54% of businesses would be interested in computer training classes.

Keya Paha/Brown/Rock Counties

The *2003 Information Technology Assessment and Plan for the KBR Region, Nebraska* focuses on telecommunications infrastructure; technology literacy and access; and economic development and e-commerce. The KBR Techknowledge Coalition will begin implementation of their plan this fall. Patty Barstow, the Executive Director of the North Central Development Center in Ainsworth contributed the following tips which were included in the revised *Community IT Planning Workbook*:

- Select committee members that are interested in technology growth.
- Have work sessions instead of meetings so you don't have to worry about quorums, etc.
- Have a large enough group to cover the members that lose interest or don't attend work sessions.
- Make sure all counties/communities are represented equally.
- Make sure all members have email and check it regularly.

- Have 2-3 hour work sessions and don't meet as often.
- Keep work sessions moving so members don't feel they are wasting time.
- Rotate meeting places between counties/communities and alternate times to accommodate members' schedules.
- Utilize e-mail for contact between work sessions.
- Conduct some work sessions via e-mail if most agenda items are following up previous discussions with research/feedback.
- Keep members well informed with work session dates/times, agendas, work session summaries, research web sites, etc.
- Request RSVP's for work sessions so you know who is planning to attend and who is reading their e-mail.
- Accept the fact that there will not be full attendance at all work sessions.
- Accept the fact that some members will lose interest.

Members from the committee were selected to represent each of the e-readiness areas. The most important thing is to have all committee members online and encourage (sometimes insist) they check their e-mail often. If you entice them with having some work sessions via e-mail they are more willing to check it regularly☺

We conducted monthly work sessions that lasted from two to three hours. The rationale for this was to accomplish lots of work with the least amount of travel time (an issue in our rural area, especially in winter). Agendas were e-mailed several days before the work session then I followed each session with an email summary of what was discussed/decided. I also sent another e-mail mid-month with a reminder of the date of the next work session. I did most of the research for the survey, etc. then e-mailed the web sites to the members so they could review them before the work session. This kept everyone up to date even if they didn't get to attend some work sessions.

We rotated our work sessions between the three counties and also alternated between afternoon and evening. About midway through the process I began requesting RSVP's to know who was planning to attend the meeting. I did this for two reasons. First, that told if some were not reading their emails. If I felt someone wasn't reading their e-mail regularly, I would call "just to update" them then casually ask them to watch for more info via e-mail. Second, it allowed me to change the meeting place, or even time, if all attendees happened to be from one community. For example if everyone coming was from Ainsworth we had the meeting here instead of everyone driving to a different town.

When working with a large group from several communities you must assume there will not be full attendance at all work sessions. I tried to keep everyone informed and encouraged them to participate with feedback and attend the community forums.

The KBR TechKnowledge Coalition 2003 Information Technology Assessment and Plan was included in the revised *Community IT Planning Workbook* as a sample plan.

West Point Area

In northeast Nebraska, West Point, Wisner, Beemer, Bancroft, Dodge, Scribner, Schuyler, Oakland, Lyons and Pender have developed a regional technology plan. The plan focuses on telecommunications infrastructure; economic development and e-commerce; and local government and community services.

Telecommunications Infrastructure. Currently some homes and businesses have cable modem, DSL or fixed wireless service available. Forming a regional technology committee has facilitated discussions with providers. The area has seen an expansion in the provision of broadband services—particularly fixed wireless service. A significant portion of the rural areas more than a couple of miles outside of the city limits cannot receive broadband services via cable modem, DSL, or fixed wireless services. The possibility of developing an engineering plan to "fill in the gaps" for high-speed Internet access was explored. Because of the complexity and costs associated with the current technologies the study was deemed infeasible. Suggested action items include meeting with public officials to discuss the problems rural communities encounter while trying to become Information Age communities; creating an online directory of information technology services available in the region; and continuing to explore ways of providing high-speed Internet access to farming and livestock operations, agribusinesses and acreages.

Economic Development and E-Commerce. There is some recognition in the area that information technology is an economic development tool. Some local businesses are using information technology effectively to improve productivity and expand markets. Surveys were conducted in Scribner and Oakland to determine how businesses in those communities were using technology. Action plan suggestions include meeting with the Department of Economic Development to better understand the needs of information-based businesses; working with high school students or a college intern to help local businesses adopt and enhance e-business applications; sponsoring e-commerce training in two communities in 2004; and coordinating a technology fair.

Local Government and Community Services. Several communities have informational Web sites, however, most are limited to economic development information. Suggested action items include offering basic computer and Internet training to county and local government officials and employees, and offering Cooperative Extension's Access e-Gov training to county and local government officials and employees.

York

After reviewing the results of a community survey, the York County has developed a draft technology plan. The plan identifies four priority areas: local government and community services; e-commerce and economic development; technology literacy and access; and leadership. Leadership development and local government services were identified as the highest priorities. The action plans for these areas are listed below:

Local Government Services Action Plan

1. Aggregate needs for agencies and build spirit of cooperation among various government entities and agencies.

2. Study current systems in place in other communities.

3. Work with entities to provide adequate budget support for implementation.

4. Ensure adequate training of public officials and end using public.

5. Encourage local governments to digitize City/County Services such as:

    - Ordinances and Forms
    - Meeting agendas and minutes
    - Entity services and/or resources online

Community Leadership Action Plan

1. Educate current and future leaders of technology advantages.
    a. Leadership York
    b. Youth Leadership York
    c. Service Clubs Education

2. Develop county-wide strategic information technology plan and share the vision.

3. Broaden representation of the Technology Committee by seeking the involvement of seniors, youth, industry, businesses, technology providers and governmental entities in committee activities.

Lessons Learned

1. Community technology planning requires a substantial time commitment from technology committee members and facilitation by energetic, committed community leaders. The mini grant program provided an incentive for communities to focus on technology planning.

2. The *Community IT Planning Workbook* simplifies the planning process. Participants liked the workbook and appreciated not having to develop their own assessment and planning tools. Participants suggested that sample plans and a glossary of technology terms be included. These changes were made to the revised *Community IT Planning Workbook*. In addition, the facilitator's guide was revised and includes tips gleaned from working with the participating communities as well as tips from community leaders. Additional worksheets to help committees plan supplemental assessment activities, build community support, develop a technology plan, and plan implementation activities were also developed. The workbook is beginning to gain national recognition as a valuable resource. The NITC has already received a request from Minnesota to use the workbook in a broadband promotion project.

3. Sometimes forming a technology committee can attract the attention of telecommunications providers, facilitating discussions between the community and providers on the availability and deployment of advanced services.

4. Documenting community needs through the assessment process can assist in the preparation of successful grant applications.

Future Plans

Six more community and regional groups are participating in the 2003-2004 IT Planning and Mini Grant Program. Ord, Homer, and Hastings have already held their initial committee meetings. Other participating communities include Dakota City, Maskell, and Lexington.

DRAFT AGENDA
(Date of last revision: September 23, 2003)

Nebraska Digital Government Summit
A Government Technology Executive Leadership Forum

November 18, 2003
The Cornhusker Hotel
Lincoln, Nebraska

7:30 am
Registration and Continental Breakfast in Exhibit Area

8:30 am
Welcome and Introductions – Lt. Governor Heineman

Opening Remarks – Governor Johanns

8:50 am
Keynote

The Point of IT All

Weary public servants can be excused for asking, "What's the point?" Legislative mandates, budgetary constraints and geopolitical threats make the hard work of doing the public's business all the more difficult. Real results in such an environment are harder to come by and require new approaches. The Center for Digital Government tracks and analyzes innovative projects nationwide. In this session, you will hear about the latest results, approaches and best practices in the use of technology in the public sector.

Paul Taylor, Ph.D., Chief Strategy Officer, Center for Digital Government

9:30 am
Plenary Panel

Meeting the Expectations of Our Customers

There have been many suggestions made as to how and where technology should be used in government. One vision has all organizations linked together in a variety of ways that provide a seamless view of government to citizens and business. We are not there yet. But where are we in the transformation from government designed for the industrial age to government designed for a mobile and global population? What should we be doing to create new models of government and governance? What is the role of technology today and tomorrow? This panel of public and private sector leaders will offer their viewpoints in an interactive and dynamic discussion.

Moderator: Scott Moore, former Secretary of State, head of government relations for Union Pacific

Panelist # 1: Bill Olson, Nebraska attorney

Panelist # 2: John Kelly, former Arizona CIO, now with Intel (suggested)

Panelist # 3: Someone from a title company or developer (suggested)

10:30 am
Morning Break and Refreshments in Exhibit Area

11:00 am
Concurrent Sessions

1) **Leading, Managing and Motivating in Challenging Times**

Government managers often struggle with the problem of how to motivate staff and raise morale. Is government really at a disadvantage compared to private industry? How does a manager maintain morale during times of change and uncertainty? This session, presented by one of our most popular speakers, covers how to build a team that works with pride, confidence and success.

Klaus Hilgers, President, EPOCH Consultants (suggested)

2) **Cyber Security Panel**

Today's hackers are smarter and share their technology with anyone who visit's their cyber café. Maintaining security is therefore a matter of cost versus benefit and accessibility. Security policies are an important component in any security plan. These policies when backed up by sound technology can give you the security you desire while allowing your employees and citizens to use the data as they require in their daily interactions with your organization. This session will discuss policy issues for cyber security and update you on some of the technology that you can deploy to protect your systems and data.

3) **Local Government Initiatives**

What is the role of local governments in meeting the demands of citizens and businesses for online access to government information and services? Topics will include E-911, electronic payment options….

Someone from Iowa County Treasurers Association (suggested)

12:15 pm
Lunch

1:00 pm
Afternoon Keynote

eCommerce for Economic Development

Representative Tom Osborne (Bruce Riker, Chief of Staff, back-up)

1:45 pm
Concurrent Sessions

1) **State Government Initiatives**
(Include presentation on new Nebraska Online contract)
Rod Armstrong (suggested speaker)

2) **Technical Architecture Issues**
How can our collective decisions on hardware, software, data, and networks make life better?

Paul Taylor, Ph.D., Chief Strategy Officer, Center for Digital Government
Two state agencies with case studies of architecture efforts in Nebraska

3) **Business Continuity**
Neither snow nor rain nor heat nor gloom of night stays these couriers from the swift completion of their appointed rounds. Business continuity has been always been an important subject. This session will focus on key areas of concern and help you in making sure you are focusing on the key areas that will allow your organization to function throughout an emergency or to recover from a variety of catastrophic occurrences.

3:00 pm
Afternoon Break in Exhibit Area

3:15 pm
Concurrent Sessions

1) **Nebraska Technology Showcase**
Technology has been used in myriad ways throughout the State of Nebraska. In this session, organizations from the State of Nebraska will present case studies of an application of technology. Attendees will learn firsthand about why the projects were conceived, what obstacles needed to be overcome, and what the results were.

2) **Wireless Technology**
Wireless technology is not just the wave of the future. It is here and being used in many bright and successful applications in government throughout Illinois and the country as a whole. This session will look at current and emerging technologies

and will cover such issues as effectiveness; costs; security concerns; integration into other applications and current applications.

3) Geographic Information Systems – New Ideas

Government entities are discovering new uses for GIS technology. The ability to combine multiple sets of information, analyze them for geographic attributes, and display the results on a map provides dynamic opportunities to improve government operations and citizen services. The purpose of this session is to learn about some of the new uses of GIS in Nebraska and the world.

Larry Diggs, Executive Director, Nebraska Association of County Officials (suggested resource)

Alternative session:

Data Sharing

- Department of Environmental Quality (with federal)
- Criminal Justice (data dictionary, data definition)

4:30 pm
Conference Wrap Up

4:45 pm
Reception in Exhibit Area

Education Council
# of the
Nebraska Information Technology Commission

*** RESOLUTION OF SUPPORT ***

The Education Council of the Nebraska Information Technology Commission, directly and indirectly representing Nebraska public and private K-12 and higher education, hereby resolves to:

- Encourage the University of Nebraska-Lincoln, the primary Internet 2 participant within the State of Nebraska, to make application to the University Corporation for Advanced Internet Development (UCAID) on behalf of the public and private educational institutions of Nebraska (K-12 school districts, Educational Service Units, Community Colleges, State Colleges, Independent Colleges and Universities) as a Sponsored Education Group Participant (SEGP) of Internet 2 in the Abilene Network;
- Encourage all of Nebraska's educational institutions to abide by the Abilene Network Terms of Participation including the Abilene Conditions of Use, which is part of the Participation Agreement;
- Encourage the education community to name one or more advanced network applications between Nebraska formal and informal educational entities and educational entities outside of Nebraska's borders;
- Assist in the identification and/or provision of three Internet2 K-20 Initiative Advisory Team members from Nebraska to attend regional and national meetings;
- Promote the inclusion and involvement of other Nebraska educational and research entities (state agencies such as NDE, Game & Parks Commission, Library Commission; museums; zoos; hospitals; and public libraries) into SEGP status;
- Work collaboratively with the University of Nebraska and other education entities to construct a cost allocation model that will ensure sustainability of Internet 2 services and participation.

The Education Council of the Nebraska Information Technology Commission directs the staff of the Office of the Chief Information Officer to send this resolution by July 31, 2003 to:
Mr. Walter Weir, CIO of the University of Nebraska
Mr. Rick Golden, Director of Networking, University of Nebraska Computing Services Network
Mr. Kent Hendrickson, Associate Vice-Chancellor for Information Services, UNL
Mr. Dale Finkelson, Network Engineer, UNL Information Services

Unanimously supported by the NITC Education Council at their July 18, 2003 meeting

State of Nebraska

Computer Network External Intrusion Security Assessment

Summary of Findings and Recommendations

August 2003

Compiled By The
Office of the Chief Information Officer
State of Nebraska
521 South 14th Street, Suite 200
Lincoln, Nebraska 68506

402.471.4385
www.nitc.state.ne.us

TABLE OF CONTENTS

BACKGROUND

The Nebraska Information Technology Commission (NITC) Security Policies (http://www.nitc.state.ne.us/standards/index.html) require an annual audit of network security. Federal regulations that govern several critical state programs also require security assessments. Independent security assessments are widely considered to be sound business practice in the information technology security field.

To begin addressing this need, the NITC awarded a grant to conduct an external intrusion security assessment of the state's network. Following a careful process to develop an RFP and select a qualified vendor, the Chief Information Officer in January 2003 awarded a contract to Omni Tech Corporation (omnitechcorp.com). The security assessment focused on Internet vulnerabilities, only. It did not involve an on-site review of security policies, interviews, evaluation of network configurations, or a test of security systems, which are elements of other types of security assessments and audits.

The project consisted of three phases. The goal of the Discovery Phase (Phase I) was to perform intelligence gathering and foot printing activities. The Scan Phase (Phase II) identified known vulnerabilities across the entire network. The Test Phase (Phase III) provided highly skilled analysis and attacks against a limited number of state agencies. A high priority of all three phases was to avoid any disruption of services.

Several activities were outside the scope of this engagement. These included war dialing, wireless security assessment, security testing of business applications, and social engineering.

This report presents the findings and recommendations from the external intrusion security assessment. It is based on the detailed technical reports submitted by Omni Tech following each of the phases. Also, on July 29, the CIO met in Milwaukee with the entire team assigned to this project. That briefing provided additional insights and suggestions for improving security of the state's network.

In computer security there are always opportunities for improvement. The purpose of this security assessment was to provide insight into existing vulnerabilities and help promote better security practices. The most important finding of this engagement was the active interest in security issues on the part of the technical staffs in many agencies.

Other Security Initiatives. The external intrusion security assessment is just one part of a long term and continuing effort to address computer security issues. Over the last three years, we have developed a comprehensive set of security policies, prepared handbooks for security officers to use in preparing security programs, and written a security incident reporting procedure. We held a Security Awareness Day on July 15, 2002, and made available a security awareness training application. Recently, the NITC adopted a set of guidelines for disaster recovery planning. Work will commence, soon, on a template for business continuity planning for state agencies. A security work group recently completed policies and guidelines pertaining to remote access and wireless security, which will be presented to the NITC for review and approval in September. More information is available at: http://www.nitc.state.ne.us/tp/workgroups/security/index.htm.

SUMMARY OF METHODOLOGY, FINDINGS AND RECOMMENDATIONS

PHASE I -- DISCOVERY

Methodology

Omni Tech Corporation performed the Phase I section of the assessment project against the State of Nebraska's registered Class B address range of 164.119.x.x. The purpose of Phase I was to identify the accessible systems from the Internet and to do preliminary footprinting of those systems. Several tools were used to do initial discovery of the State's Internet presence, including but not limited to; ARIN, NMAP, SecureScan NX, Telnet, ping, and nslookup. Also, the IP range's registration was verified using the Whois database.

Omni Tech Corporation discovered 1,545 hosts that responded in one way or the other to its tools. The number of discovered devices indicated the expected configuration of most hosts being filtered from the Internet by firewalls and other perimeter devices.

Phase I also involved scanning for open ports. There are a possible 65,535 ports on every system. These ports can be associated with services that can be accessed from the Internet. HTTP, for example, is a common service used by web pages. The "standard" port for HTTP is port #80. This process involves attempting to make a connection with the host on a number of ports. During Phase I, Omni Tech Corporation scanned ports 1-1024, 1080, 1433, 3100, 3389, 5900, 8000, and 8080. The decision was made to scan a limited number of ports to minimize the possibility of interruption of services. In Phase II and III more aggressive scanning may be performed to further interrogate systems for "non-standard" configurations.

During the initial phases no Intrusion Detection Systems (IDS) were observed. No active searches were made for IDS systems and the network discovery went as anticipated. A typical indication of an IDS system would be loss of connectivity to systems in a range of IP addresses protected by such a system. Typically IDS or shunning firewalls can be configured to ignore traffic from devices suspected of hacker-like activity (usually port scanning).

A sampling of mail servers was checked against several "blacklist" servers for spam relay identification. Blacklists are services, which identify known or suspected offenders of email abuse. Many mail systems rely on these lists to identify spammers and block email from these addresses. None of the IP addresses tested was identified as spam relays.

Findings and recommendations of Phase I include:

1. Turn off "ping" at the firewall, because responding to a ping makes it too easy for a hacker to conduct a discovery sweep.

2. Some of these devices are configured to respond to a port scan with a reset, as opposed to a timeout (the preferred configuration from a network security perspective). While this is not a risk per-se it does indicate a possible configuration issue that should be investigated. The more work an intruder has to do to map a network the better. If a host responds with a reset it is a definite indication that a host exists and more investigation is warranted. If a port scan times out, it takes much longer and leaves doubt to whether a host is there or not.
3. The number of devices configured to the Internet is probably too large. PCs, printers, copiers, and other devices should not be configured to the Internet. In general, the only hosts that should be configured to the Internet are those needed for serving content.
4. Numerous hosts were discovered to have unneeded services running that could indicate vulnerable systems. These unneeded services should be turned off, because they give the potential hacker too much information, and there is always the potential for new vulnerabilities targeted to a particular service. Options include blocking everything at the firewall at the perimeter AND turning the services off at the host level. Outdated or non-standard configurations were also noted, and several services were discovered running on non-standard ports, which could indicate a security issue or an improper configuration. These unneeded services are listed in Appendix A.
5. Consider Intrusion Detection System (IDS), AFTER the range of targets is narrowed. Fix network holes first, otherwise the volume of IDS alerts is unmanageable. Use IDS on the inside of the firewall to record events that should not have happened. Configure the IDS to watch for specific things on specific servers.

PHASE II -- VULNERABILITY SCAN

Methodology

Omni Tech Corporation conducted a limited scan using automated tools such as Retina, Nessus, and SecureScanNX. "Limited" means that any known-to-be-dangerous tests were not used. In addition, Omni Tech Corporation managed both the depth and aggressiveness of the scans to minimize the risk of disruption.

The decision was made that Phase II targets would be broken up along Class C lines for easier report dissemination by agency and to distribute the traffic on the State’s network. These guidelines were followed with the exception of the 164.119.9.x and 164.119.10.x networks, which are not “assigned” to an individual agency, but are broken up into many agencies. The .9 and .10 subnets were broken out by agencies, as identified by the Division of Communications and Information Management Services Division.

Any scanning tool will miss certain vulnerabilities. These “false negatives” may result from something as simple as a service not being available at the time of the scan. Additionally, it may be because of the conservative settings chosen to prevent the risk of service disruption. Any scanning tool will report vulnerabilities, which do not actually exist. These “false positives” may result from something as simple as a service that provides misleading version information. If a host in Phase II is identified with a vulnerability, manual verification may be necessary to verify the accuracy of the report.

Out of 1545 hosts identified in phase I, a total of 2765 vulnerabilities were found. 139 hosts are likely to contain “high risk” vulnerabilities, 1186 are likely to be susceptible to “medium risk” vulnerabilities and 1429 may contain “low risk” vulnerabilities. These figures represent the total number of incidents in each category of risk. Many hosts had multiple vulnerabilities. Three agencies had no high or medium risk vulnerabilities. Agencies that do not address network vulnerabilities pose a threat to other agencies on the network and to agencies that share services.

Omni Tech defines “high risk vulnerabilities” as a flaw in the system or configuration, which by itself may give an attacker direct access to manipulate information. Medium risk is defined as a flaw in the system or configuration which, when combined with other vulnerabilities or information, may provide access to information. Low risk is considered a vulnerability that discloses configuration information about a host. The information provided is not required for the application to function and provides an attacker with unnecessary “target definition” data.

Overall risk also depends on whether a system is critical and whether multiple risks exist that magnify the potential for problems. Combining several lower risk vulnerabilities on a server with "interesting" data may create sufficient incentive and enough holes for a hacker to compromise the system. The ability to compromise one server on the network and use it as a base of operations to attack other servers on the network can also magnify the significance of vulnerabilities on the target server.

Phase II confirmed the finding of too many hosts and too many open ports and services exposed to the Internet. This problem was widespread but especially serious in a few agencies. Appendix B lists some of the more critical vulnerabilities.

During the course of defining the targets for Phase II, it was discovered that there is no “centralized” authority for the identification of IP addresses assigned to State agencies. This became very problematic when it came time to identify the targets of the vulnerability scan, as it was the State’s desire to have individual reports for each agency. Several lists were provided to identify the mappings of IP address to hosts belonging to State agencies, but these lists were out of date and inaccurate. At the conclusion of Phase II it is unreasonable to assume that the targets addressed by the scans are inclusive of each State agency. Some systems surely have been overlooked.

Findings and recommendations of Phase II include:

1. There are too many hosts, open ports and unneeded services exposed to the Internet. This gives potential hackers too much information and there is always the potential for new vulnerabilities targeted to particular services. The state should adopt a stringent test for opening a port and services: "what is the compelling reason for the service?" If a compelling case does not exist, the default should be to shut off the port and service.
2. Complete and accurate information on the assignment of IP addresses does not seem to exist. Network maps and network diagrams are important tools for managing networks, including understanding what systems are critical, determining network configuration, and responding to problems. Require IP registration of all devices configured on the network. Information should include the IP address, type and function of the device, agency, and contact person. A network map and diagram should show the connections of all devices and identify what assets need the highest levels of protection. Registration should start with a high-level, simple database that focuses on mission critical devices.

3. A significant number of potential vulnerabilities exist. It is important to eliminate existing vulnerabilities. This should include:
    - 3.1. Address high risk vulnerabilities at the host level;
    - 3.2. Configure the firewall to restrict traffic for some services to a specific host, if there is a valid reason to keep that service open.
    - 3.3. Focus on the total number of open services and vulnerabilities as the measure of progress, not just high-risk vulnerabilities.
4. The State should establish an expectation that vulnerabilities should be an aberration. There should be a continuous effort to identify and eliminate vulnerabilities now and in the future. The strategy should include keeping patches current and adopting sophisticated firewall management, including an application firewall in some situations.

PHASE III – TESTING AND VERIFICATION

Methodology

Omni Tech Corporation performed Phase III of the security assessment project for the purposes of testing and verification. Phase III also served to demonstrate the potential consequences associated with vulnerabilities. Pursuant to the terms of the engagement, testing and verification focused on a subset of agencies. The CIO identified 19 agencies for inclusion in Phase III, based on several criteria: number of vulnerabilities, agency desire, and risk profile of the agency. Omni Tech Corporation determined which servers to attack in each agency, based on vulnerabilities and apparent value of the asset.

Omni Tech Corporation analyzed the results of Phase II as a starting point for Phase III. High and medium risk vulnerabilities were analyzed for suitability for exploitation. Phase III also investigated the possibility of exploiting other available services that Phase II did not initially identify as being subject to attack. Exploits may exist for some of these services, or they may provide information about the target that can be used by a hacker in other ways.

The actual number of hosts tested was reduced based on the availability of vulnerabilities and the functionality of the host. While the primary target may have been a high profile host, such as a Web server, the possibility of exploiting lesser hosts that may lead to more important hosts was also investigated.

Omni Tech Corporation conducted Phase III with significant constraints to avoid any disruption of service. Constraints included taking no action that would crash a system, only using tools that have been proven to be safe, not engaging in destructive testing, not mounting denial of service attacks, and not modifying nor deleting data. As conducted, Phase III activities represent the initial research for a full penetration attack or social engineering.

Omni Tech Corporation combined the results of individual scans for each agency participating in Phase III to generate an agency view of vulnerabilities discovered, available services, and open ports. The methodology then used the following steps:

1. Target selection was based on the Phase II results.
   1.1. High and medium risk vulnerabilities detected.
   1.2. Web servers with the potential for interesting data.

2. Manual verification of High and Medium risk vulnerabilities.
   2.1. Verified through extended data on Phase II report. (Extended data is the information returned by the scanning tool as a result of a test case being run; e.g., banner information from a web server that identifies its version.)
   2.2. Verified using a separate tool. (Telnet, GetIF, Browser, etc.)
   2.3. Not all vulnerabilities could be verified without an exploit or crashing the host.
   2.4. Tools used during testing were limited to trusted sources. In the case of open source tools, source code was analyzed to prevent any unknown additional effects such as Trojans or malicious applications.
   2.5. Web server source code was analyzed to provide information regarding the web applications running on a server, i.e., Cold Fusion, Active Scripting Pages, CGI scripts.

The scope of the project for the State of Nebraska was that of an assessment. The project did not include a penetration test which would have taken all the data thus far and investigated the possibility of compromising hosts on the inside of the State's network. Much of the data collected and vulnerabilities discovered would have provided many opportunities to compromise more of the State's network. Several hosts revealed valuable data for social engineering, which is often a component of penetration testing.

Findings and recommendations of Phase III include:

1. Three servers were compromised to the point of ownership (owned in hacker terms) meaning the ability to perform any functions desired on the device. These are most probably not the only hosts subject to compromise. There were many other vulnerable hosts that have exploits which are either not available (unpublished) or could not be found. We felt that this does not make the host secure, it merely means that given the scope of the project we where not able to exploit the vulnerabilities.
2. Fifty-five vulnerabilities were verified in the 19 agencies tested. These do not include low risk vulnerabilities, which are typically banner (informational only) or simple TCP services (which were detailed in Phase I).
3. A noticeable number of vulnerabilities have been addressed by some agencies. By verifying the Phase II results we were able to determine that several vulnerabilities have been addressed.
4. While the majority of the vulnerabilities were unable to be exploited, this does not mean that a problem does not exist. A determined intruder could still potentially exploit these issues by using tactics or exploits that Omni Tech Corporation could not use under the terms of the engagement. The important thing to keep in mind is that every hole (vulnerability, service, application) provides an intruder with another way into the network. Even low risk vulnerabilities (such as simple TCP services) can assist an intruder in attacking a network.
5. It was apparent that many agencies are not filtering traffic, which compounds the issue of extra services and out of date applications. If basic filtering were in place the majority of vulnerabilities would not have been revealed from the external network. While filtering external traffic does not resolve the vulnerability, it does reduce the risk profile from the majority of networked systems (Internet).

CONCLUSIONS

It appears that the agencies addressed many of the findings from Phase II once they received the reports. Many of the hosts had been removed from the Internet or blocked using a firewall or similar filtering device. A substantial number of vulnerable hosts still existed in agencies participating in Phase III, which reflects just a percentage of the overall hosts in Phase II.

We believe that this project has raised awareness in the State to the existing issues that could lead to compromised information on the network. Such compromises may have already occurred. The best way to assure no further compromises would be to follow the "least privileged" mode of operations. Multiple layers of filtering would also prevent any compromise from spreading into other departments.

Further testing on the hosts that have been identified as vulnerable should be performed to insure that the identified vulnerabilities no longer exist.

A procedure should be adopted to prevent future vulnerable hosts from being placed on the State's network to minimize the risks. This procedure should include documentation and testing of the latest patches and security fixes being applied before hosts are allowed on the Internet. Testing of hosts should also occur on a periodic basis to assure that no changes have been made that could open new holes on a host.

Segmentation of the State's network will help minimize the possibility of an intruder compromising one agency and moving on to other connected agencies. Firewalls or other filtering devices should be in place to separate the different agencies, providing another layer of protection from attack.

Filtering traffic at many layers would also improve the risk profile of the State's network, assuring that if an agency neglects to address an issue the filtering could take place at another layer of the State's network. Currently a majority of the host on the State's network responds to a PING request (ICMP echo). This service is not typically necessary and only assists an intruder in mapping the network. Filtering ICMP traffic would be the most effective way of reducing this exposure.

Mapping the State's network from a visual standpoint would greatly assist in designing a more secure network. Visualizing the network requires a deeper knowledge of the IP addressing scheme and also shows the possible connection points between agencies (such as shared systems).

APPENDIX A

LIST OF UNNEEDED SERVICES (PHASE I)

Services listed below are typically considered to be inappropriate for external access. The detailed report lists the host on which these services can be found.

From an information security view, it is recommended to close all ports that are unneeded to secure the system from known and unknown attacks. The following ports should be disabled if possible, or access to these ports should be controlled at the router or firewall to limit the exposure to the greatest extent.

- CableRouter: The following IP addresses may have a Linux remote desktop service running on port 1024. The PAM console module in Linux systems allows a user to access the system console and reboot the system when a display manager such as gdm or kdm has XDMCP enabled. (4 IP addresses)
- Cachefsd: The CacheFS file system is a general purpose caching mechanism that improves NFS server performance. CacheFS is a “helper service” and is not needed on the external network. (1 IP address)
- Chargen: A character generator service used for troubleshooting. Unnecessary service that can be used to attack systems. (43 IP addresses)
- Daytime: A service that provides the current time. The service can be exploited to cause a “denial of service” attack. Typically not used. (42 IP addresses)
- Discard: The discard service basically throws away any data sent to it. There is no practical use for this service. (51 IP addresses)
- Echo: As the name implies, any data sent to this port is “echoed” back to the requestor. This service can be used for “denial of service” attacks and should be disabled. (58 IP addresses)
- Epmap: End-point mapper helper service typically used for LAN-based Windows networking. (118 IP addresses)
- Famrpc: RPC helper service with no valid use. Should be disabled. (1 IP address)
- Finger: A simple service that can remotely identify users who are logged in. (36 IP addresses)
- Gopher: A predecessor to HTTP. This service is outdated and no longer used. (8 IP addresses)
- LanMan: Windows LAN Manager service. An outdated security service, which should be upgraded to a more secure mechanism. (95 IP addresses)
- Mountd: Daemon used to “mount” or map drives on remote systems. This service is highly insecure and can be easily tricked. (4 IP addresses)
- Ms-sql-s: SQL database service provides direct access to the database and should not be available to the Internet. (32 IP addresses)
- NetBios Name: The Netbios service should not be made available to the Internet, because it discloses information about systems. (7 IP addresses)
- NetBios Session: The NetBios service should not be made available to the Internet, because it discloses information about systems. (97 IP addresses)
- Nfs: The Network File System (NFS) is a client/server application that lets a computer user view and optionally store and update files on a remote computer as though they were

on the user's own computer. NFS has known insecurities and should not be used on the public network (2 IP addresses)

- Nlockmngr: An NFS helper service used to lock volumes. Should be disabled along with NFS. (4 IP addresses)
- Pop2: Post Office Protocol 2 is a simple mail protocol not typically recommended due to the weak authentication mechanism. (1 IP address)
- Pop3: Post Office Protocol 3 is a simple mail protocol not typically recommended due to the weak authentication mechanism. (39 IP addresses)
- PortMapper: This service “advertises” the other services available from this host. It should be blocked from the outside. (19 IP addresses)
- Printerd: (Printer ports found) The following list of IP addresses was found to have a printer configured. It is not typically expected to see printers on the outside of the network. This may indicate a configuration issue with a filtering device or the placement of the device may be insecure. (36 IP addresses)
- Quote (quote and rquotad): Quote of the day service, sends a short message to clients when they login. There is no production value in this service. (31 IP addresses)
- Rlogin and rsh: R-services or remote services are insecure protocols and should not be used. There are acceptable replacements for these services that provide the same functionality securely. (11 IP addresses)
- RTSP: Real time streaming player. This could be a legitimate server for serving up real time video or audio. (1 IP address)
- Remote Access (Timbuktu, VNC Server, and Windows_TerminalServer4): Several ports were identified which could potentially be used to remotely access machine and take over full control. These types of services are not generally recommended on external facing machines due to the risk of unauthorized access. If remote access is necessary it is recommended that the traffic would be tunneled through an encrypted connection such as VPN. (88 IP addresses)

APPENDIX B

LIST OF CRITICAL VULNERABILITIES (PHASE II)

1. SNMP Available.

Simple Network Management Protocol is a service that provides read and write capabilities over a network which allows for remote management. SNMP was a "temporary" protocol developed in the earliest stages of what we now know as the Internet. The protocol was not intended to be used in production environments; therefore no real security features were designed into the protocol. All traffic travels in "clear text" meaning it can easily be intercepted and captured or manipulated. The only form of security available is known as a "community string." This is a simple password assigned by the administrator. Unfortunately, this information also travels in the clear and is easily intercepted. At a minimum all SNMP traffic (port 161 UDP) should be blocked at the perimeter of the State's network. All hosts identified should be configured with an access list of authorized hosts if SNMP is found to be necessary. Configuration of the default community strings should also be modified with a difficult to guess password to prevent the casual intruder from gaining access by luck. The service should also be configured for "read only" to prevent anyone from making changes to systems without authorization. The chart below reflects that the majority of all vulnerabilities are related to port 161, which is the default port for SNMP. The biggest impact on the number of vulnerabilities can be realized by addressing this issue.

2. Telnet and FTP

A total of 79 hosts were found to be running Telnet and 89 hosts were running FTP. These protocols are considered insecure and should be replaced by secure shell and secure copy. It was also observed that several services are running on non-standard ports, which is not a known vulnerability, but may indicate a situation where the service is unauthorized and is trying to avoid detection by running on a non-standard port. The systems running telnet on 2001, 6001, and 9001 are most likely Cisco devices. These may be configured as "reverse telnet" ports, which may allow the devices to be used as hopping points for hackers.

3. Unnecessary Ports

As we discovered in Phase I, many hosts have ports and services running that are unnecessary. These services can be used to gather information or disrupt services on systems running on the Internet. The best practice would be to remove or disable these services from the host themselves, but a temporary fix would be to restrict traffic at routers to limit traffic to approved protocols.

A large number of ports were found to be open on many systems. This indicates a larger problem with the configuration of the State's wide area network and filtering procedures. Best security practices recommend that only "authorized" traffic should be allowed to pass through perimeter filtering devices (routers, firewalls, etc) to limit the possible points of attack. There are many benefits to this method including the prevention of unauthorized systems communicating outside the State's network. If a procedure is implemented that explicitly denies all traffic a greater amount of control and understanding can be gained about the State's network. A change control system should include a method of tracking, the purpose of the traffic rule, and an authorization mechanism to provide for checks and balances.

4. Web Server Vulnerabilities

The second highest number of vulnerabilities was associated with port 80, which is the default port for HTTP traffic. This would be expected due to the high percentage of Web servers on the

Internet. Patching the applications and adjusting the configurations can mitigate these vulnerabilities. The HTTP and HTTPS protocols were also identified on many other ports, which is not a vulnerability, but may indicate a situation where the service is unauthorized and is trying to avoid detection by running on a non-standard port.

5. Internet Relay Chat
Ten (10) hosts where found to be running IRC. This chatting protocol is associated with hackers and illegal software distributors. IRC consumes bandwidth and does not have a typical business use. The State expressed an interest in identifying hosts running this protocol as it has been discovered in the past on hosts that have been compromised.

6. MS-SQL Port 1433
Twenty-six (26) hosts were found with port 1433 open, and this indicates that an instance of Microsoft's SQL database server is running on these hosts. The recent SQL Slammer worm caused disruptions on the Internet due to un-patched servers with this port open to the outside world. There is typically no reason to offer this service to the external network and this port should be blocked.

7. TFTP Port 69
Ten (10) hosts were found to be running Trivial File Transfer Protocol. TFTP can be dangerous to systems because there is no authentication mechanism in place. If a host is running TFTP an attack only needs a client to place or retrieve files from a system. This protocol should be removed or blocked.

8. Outdated operating systems
Several hosts have been identified running MS-Windows NT that is at the end of life for Microsoft. Several vulnerabilities have been identified on hosts running this operating system, some of which can not be addressed by normal patching. The applications running on these hosts are in danger of being compromised. The best approach would be to upgrade or replace the systems that are running older operating systems.

One agency in particular has hosts with outdated operating systems. Through the course of Phase II testing, several issues were uncovered with the web server supporting this agency. The agency was notified and chose not to resolve the issues as they are migrating their platform to the Nebraska Online facility.

Several versions of the Linux kernel were also identified. Older versions of the open-source operating systems have known flaws, which can lead to the compromise of the system.

9. Scanning traffic blocked
On a few occasions traffic from the Omni Tech Corporation facility was blocked by the IS staff. The amount of traffic being generated into the logging system was slowing down the network to the point that people were complaining. The choice was made to block the traffic. Unfortunately, no notification was made to Omni Tech Corporation and it took several days to clear up the issue. A more suitable resolution would have been not to log the traffic from Omni Tech Corporation and allow testing to continue. In the future if testing on a large scale will be performed a notification method should be established and the proper log file configuration should be agreed upon before such testing begins.

10. Other High Risk Vulnerabilities
A summary of high-risk vulnerabilities and the frequency of each includes:

High Risk Vulnerability	Total Servers	Total Agencies
Active SNMP Agent	79	12
Apache HTTP Server Chunked Encoding Buffer Overflow	8	6
BIND SIG Cached Resource Record Overflow	3	3
FormMail CGI	1	1
HTTP DELETE Method Allowed	1	1
HTTP PUT Method allowed	1	1
Imapd Buffer Overflow	2	2
IPSSWITCH IMail File Attachment	1	1
ISC Bind 8 Transaction Signature Buffer Overflow	1	1
Lotus Domino Authentication Bypass	1	1
Microsoft ADCTEST.ASP Sample File	3	3
Microsoft SQL Server Weak Authentication	11	7
Multiple Vendor BIND NXT Overflow	1	1
NFS Export is Writeable	1	1
NFS Mountable Volume List	1	1
O'Reilly WebSite 'webfind.exe' Buffer Overflow	2	2
O'Reilly WebSite GET Buffer Overflow	2	2
Piranha Linux Virtual Server Default Password	1	1
RDS/IIS	5	5
Rexec Service is Running	2	2
Rsh Service is Running	1	1
SSH CRC-32 Compensation Attack Detector	1	1
TFTPD32 Arbitrary File Download/Upload	2	2

APPENDIX C

LIST OF AGENCY REPORTS FOR PHASE II AND PHASE III

(For access to the reports, contact Doug Hahn at IMServices – 471-9578.)

Agency	Phase II	Phase III
Coordinating Commission for Higher Education	X	
Crime Commission		X
Department of Correctional Services	X	X
Department of Economic Development	X	X
Department of Education	X	X
Department of Environmental Quality	X	X
Department of Health and Human Services	X	X
Department of Insurance	X	
Department of Labor	X	X
Department of Motor Vehicles	X	
Department of Natural Resources	X	X
Department of Property Assessment and Taxation	X	
Department of Revenue	X	X
Department of Roads	X	X
Division of Communications	X	X
Game and Parks Commission	X	
Information Management Services Division	X	X
Legislative Council	X	X
Library Commission	X	X
NDE – Assistive Technology Partnership	X	
NDE – Developmental Disability	X	
Nebraska Information System	X	
Nebraska Online		X
Public Employees Retirement Systems	X	X
Secretary of State	X	X
State College System	X	
State Personnel	X	
State Surveyor	X	
State Treasurer	X	
Workers Compensation Board	X	

Statewide Technology Plan
Update on Action Items
September 23, 2003

The NITC has prepared an action plan consisting of twenty items which address the NITC's four goals of supporting the development of a robust telecommunications infrastructure; supporting community and economic development; promoting the efficient delivery of government and educational services; and promoting effective planning and accountability. The current status of the NITC's 2003-2004 action items is listed below. A brief description of each action item is available on the NITC home page: www.nitc.state.ne.us.

Action Items	**Status as of September 2003**
Telecommunications Infrastructure	
1. Provide technical assistance for the Collaborative Aggregation Partnership for the development of statewide network services (TP 1.1)	Phase I (Kearney, Grand Island, Omaha and Lincoln – October 1, 2003 implementation Phase II (Norfolk, North Platte, Panhandle) – January 31, 2004 implementation.
2. Provide technical assistance for aggregation and consolidation of networks (TP 2.2)	Technical assistance for the statewide network is being provided through the Collaborative Aggregation Partnership (CAP) group. (See below for status of efforts on statewide synchronous video.)
3. Support the Nebraska Network through the Network Policy Work Group (CC 3, EC 1.2, SGC 2.3)	The Interim Network Policy Work Group has met twice (August 1 and September 3). A customer information manual, customer agreements, and other steps are underway. The next meeting is September 24.
4. Determine statewide synchronous video network requirements (TP 2.2.1, EC 1.1)	The Statewide Synchronous Video Work Group has met three times (March 26, May 28, July 30). A comprehensive update was provided to the Public Service Commission on August 26, 2003 and a list of five first-round recommendations are ready to present to the Technical Panel on September 17 and the NITC on September 30.
5. Support the development of the Nebraska Telehealth Network (CC 2)	With support from the Bioterrorism Executive Committee, the Nebraska Hospital Association is including bioterrorism response in their next phase of planning. Discussions continue with the Public Service Commission and hub hospitals on the development of a telehealth network.
6. Address the need for sufficient rural bandwidth EC (1.2)	Educational delegates from rural areas are participating on the Interim Network Policy Work Group, the Statewide Synchronous Video Work Group, and at least one person from the Panhandle is assisting with the evaluation of Phase2 Netcom bids. The Education Council task group to concentrate on this issue will be named at their meeting on September 19, 2003.

Community and Economic Development	
1. Encourage and support community IT development (CC 1)	• Communities participating in the first year of the IT Planning and Mini Grant program are completing their technology plans and beginning implementation. • An expanded Community IT Planning Workbook has been developed. • TANgents, a quarterly electronic newsletter from Technologies Across Nebraska, reaches nearly 1,500 individuals. • Homer, Dakota City, Ord, Lexington, Maskell, and Adams County are scheduling initial community meetings and will begin developing technology plans through the 2003-2004 IT Planning and Mini-Grant program.
Efficient Delivery of Government and Educational Services	
1. Determine the business case for reinstatement of the Technology Training Grant Fund (EC 2.1)	The Education Council task group to concentrate on this issue will be named at their meeting on September 19, 2003.
2. Support the Nebraska eLearning Initiative (EC 5.1)	The Nebraska eLearning Initiative has been named as one of the five project components of the Network Nebraska implementation. A project team has been named to pursue sources of grant funds.
3. Assist in the development of value-added services for the Nebraska “Click into Education” portal (EC 5.2)	Of the three projects prioritized by the Education Council: Statewide admission form, searchable database of I.T. training opportunities, and searchable database of higher education courses and programs, progress is being made on each through the cooperation of Nebraska OnLine and the staff of the NITC.
4. Study and promote effective synchronous and asynchronous instructional methods (EC 6.1)	The Education Council task group to concentrate on this issue will be named at their meeting on September 19, 2003.
5. Implement *E-Government Strategic Plan* (SGC 1.1)	Of the 26 specific “Actions and Recommendations” contained in the Plan, 15 have either been completed or progress is being made. The remaining 11 have yet to have significant progress made.
6. Develop guidelines for electronic records retention (SGC 2.2)	The SGC created a work group which drafted a best practices resource document for the retention of Lotus Notes e-mail and related documents.
7. Recommend technical standards, guidelines, best practices, and enterprise solutions (TP 2.1, SGC 2.1)	Recommendations completed for: E-fax Guideline; Wireless Local Area Network Guidelines; Remote Access Guidelines; Lotus Notes E-mail Retention Best Practices; and Directory Services Work Group Recommendations. Work is progressing on: Blocking E-mail Attachments Guideline; Blocking SPAM Guideline; and Internet .GOV Domain Naming Convention. A work group is

	reviewing the E-mail Standard for State Government; and IMServices is coordinating meeting with agencies to identify other areas which will benefit from standards and guidelines.
Planning and Accountability	
1. Improve planning process and project management (SGC 3.1)	Work not scheduled to begin until the 4th Quarter of 2003.
2. Communicate with policymakers (SGC 3.2)	Ongoing.
3. Develop and implement security policies (SGC 4.1)	Additional security policies drafted for Wireless Local Area Networks and Remote Access.
4. Conduct project reviews—statutory (TP 3.1)	None.
5. Conduct project reviews—other (TP 3.2)	None.
6. Revise procedures for reviewing IT projects and purchases by state agencies (TP 3.3)	Work scheduled to begin during 3rd Quarter.

*Action items were prepared and recommended by the NITC's advisory groups. Numbers refer to the identification of the action item on the advisory group's action plan. The following abbreviations are used to indicate advisory groups:

CC	Community Council
EC	Education Council
SGC	State Government Council
TP	Technical Panel

Nebraska Information Technology Commission
EDUCATION COUNCIL

Membership Replacements pending NITC approval
as forwarded by the Education Council 9-19-03

HIGHER EDUCATION NEW MEMBERS

Nominee	*Representing*	*Comments*
Arnold Bateman **alt. Kent Hendrickson**	**University of Nebraska**	**Replacing Perlman** **2002-04**
Yvette Holly **(alternate to be named)**	**University of Nebraska**	**Filling vacancy** **2003-05**
Dennis Linster **alt. Curt Frye**	**State Colleges**	**Replacing Stearns** **2002-04**

Brief Bio for Mr. Arnold Bateman, University of Nebraska-Lincoln

Arnold Bateman has been involved in extended education and outreach for the University of Nebraska-Lincoln since 1987. In 2002, he was named as Associate Vice Chancellor for Extended Education and Outreach where he provides leadership in the development of the vision and planning for the future of extended education at UNL. Mr. Bateman is UNL's chief spokesperson and representative to Central Administration on extended education and outreach issues and provides leadership to the UNL Extended Education Academic Council and Extended Education Statewide Advisory Council. His primary responsibilities include providing administrative leadership to facilitate the offering of UNL's off-campus educational and outreach programs, in consultation with respective colleges and divisions.

Brief Bio for Ms. Yvette Holly, University of Nebraska Medical Center

Yvette Holly is an experienced senior level information technology professional with over 18 years of service in an academic health sciences environment. Currently she serves as Assistant Vice Chancellor for UNMC's unit of Information Technology Services where she is responsible for the provision of data, voice and video services to the University of Nebraska Medical Center, as well as to UNMC's partner organization, Nebraska Health System. Ms. Holly's professional experience includes strategic and tactical planning; budget preparation and administration; contract negotiations; project management and personnel management; and leadership and management of large-scale, complex data and voice networks.

Brief Bio for Mr. Dennis Linster, Wayne State College

Dennis Linster has worked in the area of computer science, network systems and information technology for Wayne State College since 1991. He currently serves as Chief Information Officer for the College where he is responsible for technology budgeting, technology project design and implementation, and is the administrative spokesperson on matters dealing with technology. He has been very active in the Midwest Higher Education Consortium (MHEC), securing preferred hardware and software pricing for educational and government entities. Most recently, he is responsible for an innovative wireless technology aggregation project for the community of Wayne.

September 30, 2003

TO: NITC Commissioners

FROM: Rick Becker

SUBJECT: **State Government Council Report**

The following is a summary of the activities of the State Government Council since the last NITC meeting:

1. STANDARDS AND GUIDELINES DEVELOPMENT

The State Government Council, working with various interested agencies, has been developing standards and guidelines in a number of areas.

- Wireless Local Area Network Guidelines
- Remote Access Guidelines
- Blocking E-mail Attachments - Draft guidelines have been written for the purpose of limiting the exposure of the state's network to virus-laden attachments.
- Blocking Unsolicited Bulk E-mail / "SPAM" - Draft guidelines have been developed to provide guidance to agencies on blocking "spam."
- Nebraska.gov Domain Naming Convention - A draft standard for using the Nebraska.gov and NE.gov domain names is under review.
- E-mail Standard - The Council created a work group to review the existing e-mail standard for state government and to make recommendations regarding revisions to the standard. The work group has met regularly and is drafting a report and recommendations.

2. RECORDS RETENTION

A work group drafted a resource document entitled "Best Practices for Management of Lotus Notes E-mail Records." The document is intended to help agencies manage the retention of public records in the Lotus Notes e-mail environment. Staff from the Records Management Division assisted the work group. The Council reviewed and accepted the document at their meeting in September.

3. DIRECTORY SERVICES

The Directory Services Work Group, created earlier this year, provides policy input to the Nebraska Directory Services team at IMServices. The Nebraska Directory Services project involves the creation of an enterprise-level directory to provide secure authentication and access to various applications and subsystems in state government. The work group meets regularly to address issues raised by the implementation team. The work group's "Phase I Recommendations" were presented to the Council in August.

NEBRASKA INFORMATION
TECHNOLOGY COMMISSION

TECHNICAL STANDARDS AND GUIDELINES

XX-XXX Wireless Local Area Network Guidelines

Category	**Security Architecture**
Title	**Wireless Local Area Network Guidelines**
Number	**XX-XXX**

Applicability

☑ **State Government Agencies**
□ All..**Not Applicable**
☑ Excluding higher education institutions..............**Standard (§1.1) and Guideline**
□ **State Funded Entities -** All entities receiving state funding for matters covered by this document.................**Not Applicable**
☑ **Other:** All Public Entities..............................**Guideline**

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of ____________.
Guideline - Adherence is voluntary.

Status	□ Adopted ☑ Draft □ Other:_________
Dates	Date: September 17, 2003 Date Adopted by NITC: Other:

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-1506(6)
http://www.nitc.state.ne.us/standards/

1.0 Standard and Guidelines

STANDARD (For state government agencies only, excluding higher education institutions.)

1.1 Registration of Wireless Devices

- All wireless network access points should be registered with the network manager for that entity. State agencies must register Wireless Local Area Networks with IMServices. Self-registration will be available through the IMServices web site (www.ims.state.ne.us). The registration process will identify: a) the physical location of the network, b) the security/firewall technologies being deployed, and c) the types of services or information that is available through the wireless LAN. IMServices reserves the right to disable network access for a device, server or LAN if adequate security for a wireless connection is not in place. Wireless services that fall within the definition of campus connection, MAN or WAN must be purchased through the Division of Communications to comply with State statutes.
- Agencies using wireless systems must develop general risk mitigation strategies for access points, users and client devices such as virus protection, password standards, and other preventative measures.
- Only approved and registered access points will be deployed within state agencies. Unapproved (rogue) devices should be removed from service.

GUIDELINES

1.2 Management and Security of Access Points

- *Physical Security*: Access points should be properly secured within a safe, adequately monitored area to prevent unauthorized access and physical tampering. Devices should not be placed in easily accessible public locations.
- *Configuration Management*: All wireless access points should be secured using a strong password. Passwords should be changed at least every six months. Administrators should ensure all vendor default usernames and passwords are removed from the device. Administration of the device should be prohibited from the wireless network.
- *Rogue Wireless LANS*: Network managers for each entity should incorporate procedures for scanning and detecting unregistered (rogue) wireless devices and access points. This requires a full understanding of the topology of the network. It also requires performing periodic security testing and assessment, including randomly timed security audits to monitor and track wireless and handheld devices.

1.3 Broadcast Security and Encryption

- Agencies deploying wireless technology should adhere to minimum encryption standards, and follow best practices for secure installations.

1.4 Access to Systems and Data

- Agencies and other entities connected to the state's network must employ adequate security to protect other systems and data connected to the state's network.
- Once authenticated to an access point, users should either be routed outside the state's firewall(s), or authenticated to the network. Just as with a wired network, state network authentication--whether enterprise-wide or agency-specific-- should satisfy prescribed login/password combinations prior to using enterprise or agency-specific resources that are not normally accessible by nodes outside the state's firewall(s).
- Access control mechanisms such as firewalls should be deployed to separate the wireless network from the internal wired network.

- As the technology permits, wireless networks should employ a combination of layered authentication methods to protect sensitive, proprietary, and patient information.

1.5 Naming Conventions

- Final device names are assigned during the registration process to avoid conflicts and confusion, and to aid in incident response and in identifying and locating wireless devices.
- If technology allows for the broadcast of a device name, standardized names should appear in the broadcast description, along with any unique identifiers assigned to the unit.

1.6 Disruption and Interference

- All newly deployed wireless technologies should satisfy all existing and future standards as required by law or established by the NITC or the Information Management Services Division pertaining to use and security of the state's network.
- An entity's network manager should resolve any conflicts between wireless devices. Priority is granted to fully supported and registered installations, except in the case of medical, safety, or emergency devices, as appropriate. For state agencies, excluding higher educational institutions, IMServices will resolve any conflicts between wireless devices, in coordination with affected agencies.

2.0 Background

2.1 Purpose and Objectives

In some situations, wireless technology offers important advantages in terms of convenience, flexibility and cost savings over other types of networking. A major disadvantage of wireless technology is its inherent security risks. If not deployed properly, a wireless local area network (LAN) offers open access to everyone in the vicinity who has a wireless card in his or her PC, laptop, Personal Digital Assistant (PDA), wireless messaging devices or other computing devices.

The purpose of these guidelines is to encourage wise decisions regarding whether and how to implement wireless technology. The primary source of these guidelines is the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce, which has issued Special Publication 800-48, "Wireless Network Security 800.11, Bluetooth and Handheld Devices," November 2002. A full copy of this publication is available at: (http://csrc.nist.gov/publications/nistpubs/index.html).

NIST Special Publication 800-48 is 119 pages long. It provides a detailed overview of wireless technology, wireless LANs, wireless personal area networks ("Bluetooth" technology), and wireless handheld devices. Anyone implementing any of these types of wireless systems should read the entire report, which is incorporated into these guidelines by reference. The following guidelines copy the executive summary and the checklist in NIST SP 800-48 that specifically pertain to wireless LANs. Parts of the Executive Summary and most of Section D are based on the National Institutes of Health Wireless Network Policy.

As a final cautionary note, the ease and convenience of setting up wireless LANs should not outweigh the responsibility of every agency to consider the "security needs of other agencies or institutions connected to the network".

In addition to following the NIST SP 800-48, any public entity implementing wireless technology should notify that entity's network manager before connecting the wireless

device to the entity's network. State government agencies, excluding higher educational institutions, must comply with notification procedures established by the Division of Communications and the Information Management Services Division, as described in Section 1.1.

These general guidelines do not replace or supercede any specific standards and procedures of operational entities, which have responsibility for managing communications networks.

2.2 Executive Summary

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders.

In additional to the inherent risks associated with any wired network, wireless technology introduces several unique vulnerabilities. Since wireless signals are radio transmissions, they can be intercepted by suitable radio receiving devices, sometimes even devices operating outside the intended service area. If data transmissions are not encrypted or are inadequately encrypted, the intercepted data can be read and understood in a matter of seconds. Any data transmission sent through the wireless network is at risk, including correspondence, usernames and passwords, financial data, and other sensitive information. Because wireless transmissions circumvent traditional perimeter firewalls, those existing protections established to prevent unauthorized access are ineffective. Advances in wireless signaling technology may increase transmission distances, further exacerbating the problem of unauthorized reception. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

Since wireless network devices operate using radio signals, their proliferation within an area can lead to Radio Frequency Interference (RFI) among these devices and other radio devices using the same frequency bands.

This document provides an overview of wireless networking technologies and wireless handheld devices most commonly used in an office environment and with today's mobile workforce. This document seeks to assist agencies in reducing the risks associated with 802.11 wireless local area networks (LAN), Bluetooth wireless networks, and handheld devices.

These guidelines recommend the following actions:

1. Agencies should be aware that maintaining a secure wireless network is an ongoing process that requires greater effort than that required for other networks and systems.

Moreover, it is important that agencies assess risks more frequently and test and evaluate system security controls when wireless technologies are deployed.

2. Agencies should not undertake wireless deployment for essential operations until they have examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations. Agencies should perform a risk assessment and develop a security policy before purchasing wireless technologies, because their unique security requirements will determine which products should be considered for purchase.

3. Agencies should be aware of the technical and security implications of wireless and handheld device technologies.

4. Agencies should carefully plan the deployment of 802.11, Bluetooth, or any other wireless technology.

5. Agencies should be aware that security management practices and controls are especially critical to maintaining and operating a secure wireless network.

6. Agencies should be aware that physical controls are especially important in a wireless environment.

7. Agencies should enable, use, and routinely test the inherent security features, such as authentication and encryption that exist in wireless technologies.

8. In addition, firewalls and other appropriate protection mechanisms, such as intrusion detection systems should be employed.

3.0 Definitions

3.1 **Access Point**. A hub or interconnect device on a Local Area Network (LAN) that supports wireless (IEEE 802.11x) devices such as laptops, PDA's, etc. In some cases, the Access Point constitutes a stand-alone LAN where only a few wireless devices that need to communicate or share resources.

3.2 **Campus Connection**. (to be defined)

3.3 **Local Area Network (LAN)**. A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. For State agencies, LANs are defined as restricted to rooms or buildings. An interconnection of LANs within a limited geographical area, such as a military base, is commonly referred to as a campus area network. An interconnection of LANs over a city-wide geographical area is commonly called a metropolitan area network (MAN). An interconnection of LANs over large geographical areas, such as nationwide, is commonly called a wide area network (WAN).

3.4 **Metropolitan Area Network (MAN)**. A data communications network that (a) covers an area larger than a local area network (LAN) and smaller than a wide area network (WAN), (b) interconnects two or more LANs, and (c) usually covers an entire metropolitan area, such as a large city and its suburbs.

3.5 **Personal Digital Assistant (PDA)**. A handheld computer that serves as an organizer for personal information. It generally includes at least a name-and-address database, a to-do list, and a note taker. PDAs are pen-based and use a stylus to tap selections on menus and to enter printed characters. The unit may also include a small on-screen keyboard that is tapped with the pen. Data are synchronized between a user's PDA and desktop computer by cable or wireless transmission.

3.6 **Smart Card**. A credit card with a built-in microporcessor and memory that is used for identification or financial transactions. When inserted into a reader, the card transfers data to and from a central computer. A smart card is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times.

3.7 **Virtual Private Network**. A means by which certain authorized individuals (such as remote employees) can gain secure access to an organization's intranet by means of an extranet (a part of the internal network that is accessible via the Internet).

3.8 **Wide Area Network (WAN)**. A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and is usually spread over a larger geographic area than that of a LAN. Note 1: WANs may include physical networks, such as Integrated Services Digital Networks (ISDNs), X.25 networks, and T1 networks. Note 2: A metropolitan area network (MAN) is a WAN that serves all the users in a metropolitan area. WANs may be nationwide or worldwide.

3.9 **Wireless Application Protocol (WAP)**. A standard for providing cellular telephones, pagers, and other handheld devices with secure access to e-mail and text-based Web pages.

3.10 **Wired Equivalent Privacy (WEP)**. Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

4.0 Applicability

These guidelines are intended to be useful to all public entities that are developing their own security policies and procedures for wireless networks. They specifically apply to state government agencies, excluding higher educational institutions.

5.0 Responsibility

5.1 **Agency and Institutional Heads**. The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs, including disaster recovery plans for information technology. The authority may delegate this responsibility but delegation does not remove the accountability.

5.2 **Agency Information Officer**. The Agency Information Officer or delegate must notify the Division of Communications and the Information Management Services Division before implementing a wireless system.

5.3 **Information Management Services Division (IMServices)**. IMServices shares responsibility with the Division of Communications for the security of the state's network. State agencies must register Wireless Local Area Networks with IMServices. Self-registration will be available through the IMServices web site (www.ims.state.ne.us). IMServices reserves the right to disable network access for a device, server or LAN if adequate security for a wireless connection is not in place.

5.4 **Division of Communications (DOC)**. DOC shares responsibility for the security of the state's network with IMServices. Wireless services that fall within the definition of campus connection, MAN or WAN, must be purchased through the Division of Communications to comply with State statutes.

6.0 Related Policies, Standards and Guidelines

6.1 NITC Security Officer Handbook (http://www.nitc.state.ne.us/standards/security/so_guide.doc)

6.2 NITC Network Security Policy (http://www.nitc.state.ne.us/standards/index.html)

6.3 NITC Incident Response and Reporting Procedures for State Government (http://www.nitc.state.ne.us/standards/index.html)

7.0 References

7.1 NIST Wireless Network Security Special Publication 800-48 (http://csrc.nist.gov/publications/nistpubs/index.html)

7.2 National Institutes of Health (NIH) Wireless Network Policy, January 24, 2003, (http://www1.od.nih.gov/oma/manualchapters/management/2807/)

7.3 Information Management Services Division, “Network Security Standards” (Draft, February 11, 2003), www.ims.state.ne.us.

APPENDIX

Wireless LAN Security Checklist

The table, below, provides a WLAN security checklist. The table presents guidelines and recommendations for creating and maintaining a secure 802.11 wireless network, based on NIST Special Publication 800-48. Most of the recommendations are "best practices", which all agencies should be followed. Items marked as "Should Consider" might provide a higher level of security, but should be weighed against other considerations.

Management Recommendations

Status	Recommendation
	1. Develop an agency security policy that addresses the use of wireless technology, including 802.11.
	2. Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.
	3. Perform a risk assessment to understand the value of the assets in the agency that need protection.
	4. Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they become available (prior to purchase).
	5. Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.
	6. Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.
	7. Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).
	8. Complete a site survey to measure and establish the AP coverage for the agency.
	9. Take a complete inventory of all APs and 802.11 wireless devices.
	10. Ensure that wireless networks are not used until they comply with the agency's and the state's security policies.
	11. Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
	12. Place APs in secured areas to prevent unauthorized physical access and user manipulation.

Technical Recommendations

Status	Recommendation
	13. Empirically test AP range boundaries to determine the precise extent of the wireless coverage.
	14. Make sure that APs are turned off during when they are not used (e.g., after hours and on weekends).
	15. Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized group of people.
	16. Restore the APs to the latest security settings when the reset functions are used.
	17. Change the default SSID in the APs.
	18. Disable the broadcast SSID feature so that the client SSID must match that of the AP. (Should Consider)

	19. Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products.
	20. Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference.
	21. Understand and make sure that all default parameters are changed.
	22. Disable all insecure and nonessential management protocols on the APs.
	23. Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy feature.
	24. Ensure that encryption key sizes are at least 128-bits.
	25. Make sure that default shared keys are periodically replaced by more secure unique keys.
	26. Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).
	27. Install antivirus software on all wireless clients.
	28. Install personal firewall software on all wireless clients.
	29. Disable file sharing on wireless clients (especially in untrusted environments).
	30. Deploy MAC access control lists. (Should Consider)
	31. Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.
	32. Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications. (Should Consider)
	33. Ensure that encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.
	34. Fully test and deploy software patches and upgrades on a regular basis.
	35. Ensure that all APs have strong administrative passwords.
	36. Ensure that all passwords are being changed regularly.
	37. Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI. (Should Consider)
	38. Ensure that the "ad hoc mode" for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.
	39. Use static IP addressing on the network. (Should Consider)
	40. Disable DHCP. (Should Consider)
	41. Enable user authentication mechanisms for the management interfaces of the AP.
	42. Ensure that management traffic destined for APs is on a dedicated wired subnet.
	43. Use SNMPv3 and/or SSL/TLS for Web-based management of APs.

Operational Recommendations

Status	Recommendation
	44. Configure SNMP settings on APs for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended.
	45. Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.
	46. Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information. (Should Consider)

	47. Consider other forms of authentication for the wireless network such as RADIUS and Kerberos. (Should Consider)
	48. Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity. (Should Consider)
	49. Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity. (Should Consider)
	50. Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features. (Should Consider)
	51. Enable utilization of key-mapping keys (802.1X) rather than default keys so that sessions use distinct WEP keys.
	52. Fully understand the impacts of deploying any security feature or product prior to deployment.
	53. Designate an individual to track the progress of 802.11 security products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology. (Should Consider)
	54. Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features. (Should Consider)
	55. When disposing access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.
	56. If the access point supports logging, turn it on and review the logs on a regular basis.

Nebraska Information
Technology Commission

Technical Standards and Guidelines

XX-XXX   Remote Access Guidelines

Category	**Security Architecture**
Title	**Remote Access Guidelines**
Number	**XX-XXX**

Applicability	☑ **State Government Agencies** □ All...**Not Applicable** ☑ Excluding higher education institutions...**Guideline** □ **State Funded Entities -** All entities receiving state funding for matters covered by this document.................**Not Applicable** ☑ **Other:** All Public Entities..............................**Guideline** **Definitions:** **Standard** - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of _______________. **Guideline** - Adherence is voluntary.

Status	□ Adopted ☑ Draft □ Other:_________
Dates	Date: August 8, 2003 Date Adopted by NITC: Other:

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-1506(6)
http://www.nitc.state.ne.us/standards/

1.0 Guidelines

1.1 All home networks connected to the Internet via a broadband connection should have some firewall device installed. Personal software firewalls installed on each computer are useful and effective, but separate, dedicated, and relatively inexpensive hardware firewalls that connect between the broadband connection and the telecommuter's computer or network can provide greater protection. Organizations should consider using both personal and hardware firewall devices for high-speed connections. When both a software personal firewall and a separate device are in operation, the organization can screen out intruders and identify any rogue software that attempts to transmit messages from the user's computer to an external system.

1.2 Web browsers should be configured to limit vulnerability to intrusion. Web browsers also represent a threat of compromise and require additional configuration beyond the default installation. Browser plugins should be limited to only those required by the end user. Active code (such as ActiveX or Java) should be disabled or used only in conjunction with trusted sites. The browser should always be updated to the latest or most secure version. Privacy is always a concern with web browsers. The two greatest threats to this privacy are the use of cookies and monitoring of web browsing habits of users by third parties. Cookies can be disabled or selectively removed using a variety of built-in web browser features or third-party applications.

1.3 Operating system configuration options should be selected or disabled as appropriate to increase security. The default configuration of most home operating systems is generally inadequate from a security standpoint. File and printer sharing should almost always be disabled. The operating system and major applications should be updated to the latest and most secure version or patch level. All home computers should have an anti virus program installed and configured to scan all incoming files and e-mails. The anti virus program should have its virus database updated on a regular basis. Another concern for many telecommuters is the surreptitious installation of spyware by certain software applications. This spyware, while usually not intended to be malicious, reports information on users (generally without their knowledge) back to a third party. This information could be general information about their system or specifics on their web browsing habits. A variety of programs are available for detecting and removing this spyware..

1.4 Selection of wireless and other home networking technologies should be in accordance with security goals. Several home networking technologies are available for telecommuters who wish to connect their home PCs together to share resources. Some of these technologies are the same as their office counterparts (e.g., Ethernet), and others are designed specifically to meet the needs of telecommuters (e.g., phone- and power-line networking). While most of these technologies can be made relatively secure, some represent a threat to security of both the home network and, sometimes, the office network. In particular, wireless networking has vulnerabilities that should be carefully considered before any installation.

1.5 Public entities should provide telecommuting users with guidance on selecting appropriate technologies, software, and tools that are consistent with the agency network and with agency security policies. Users have many approaches to choose from in establishing an off-site office. Sophisticated technologies such as virtual private networks (VPNs) can provide a high level of security, but are more expensive and complex to implement than other solutions. Whenever practical, agencies should provide telecommuting users with systems containing pre-configured security software and necessary hardware. If possible, agency security administrators should update and maintain the systems as well, to minimize reliance on users who are not specialists in security features. (It is not always financially or logistically practical for agencies to provide users with pre-configured systems, and this recommendation should not be taken as a requirement of this publication.) Many users, particularly if they do not require interactive access to agency databases, can obtain an adequate degree of security at very low cost and with little additional software, easing burdens on both the user and system administrators at the central computing system. The benefits and risks of telecommuting are here to stay. Computing resources and access to office networks while on the road or working from home is too valuable for most organizations or employees to give up. While there will always be risks associated with remote access to an organization's resources, most of these risks can be mitigated through careful planning and implementation. By the same token, even though broadband connections generally represent a greater threat than dial-up connections, the threat can be reduced through careful configuration and the judicious use of the security tools and techniques discussed in this document.

2.0 Background

2.1 Purpose and Objectives

This document sets forth policies and guidelines for acquiring and managing resources used for remote access to the state's network. The following guidelines copy the Executive Summary and other information from the National Institute Standards and Technology (NIST) Special Publication, 800-46, "Security for Telecommuting and Broadband Communications". A full copy of this publication is available at: (http://csrc.nist.gov/publications/nistpubs/index.html).

Anyone implementing remote access should read the entire NIST Special Publication, 800-46, which is incorporated into these guidelines by reference.

These general guidelines do not replace or supercede any specific standards and procedures of operational entities, which have responsibility for managing communications networks.

2.2 Executive Summary

Telecommuting has become a popular trend in the workplace. As employees and organizations employ remote connectivity to corporate and government networks, the security of these remote end points becomes increasingly important to the overall security of a network. Accompanying and contributing to this trend is the explosive growth in the popularity of broadband connections for telecommuters. These developments complicate the process of securing organizational and home networks. This document assists organizations in addressing security issues by providing recommendations on securing a variety of applications, protocols, and networking architectures. Recommendations in this publication are designed for State government agencies, educational institutions and other public entities, but may be useful to commercial organizations and home users as well. Home broadband architectures face a variety of threats that, while present on dial-up connections, are easier to exploit using the faster, always-on qualities of broadband connections. The relatively short duration of most dial-up connection makes it more difficult for attackers to compromise telecommuters dialed-up to the Internet. "Always on" broadband connections provide attackers with the speed and communications bandwidth necessary to compromise home computers and networks. Ironically, as governmental and corporate organizations have hardened their networks and become more sophisticated at protecting their computing resources, they have driven some malicious entities to pursue other targets of opportunity. Telecommuters with broadband connections are these new targets of opportunity both for their own computing resources and as an alternative method for attacking and gaining access to government and corporate networks.

State agencies and their employees can take a variety of actions to better secure their telecommuting and home networking resources.

3.0 Definitions

3.1 **Access Point**. A hub or interconnect device on a Local Area Network (LAN) that supports wireless (IEEE 802.11x) devices such as laptops, PDA's, etc. In some cases, the Access Point constitutes a stand-alone LAN where only a few wireless devices that need to communicate or share resources.

3.2 **Local Area Network (LAN)**. A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. For State agencies, LANs are defined as restricted to rooms or buildings. An interconnection of LANs within a limited geographical area, such as a military base, is commonly referred to as a campus area network. An interconnection of LANs over a city-wide geographical area is commonly called a metropolitan area network (MAN). An interconnection of LANs over large geographical areas, such as nationwide, is commonly called a wide area network (WAN).

3.3 **Metropolitan Area Network (MAN)**. A data communications network that (a) covers an area larger than a local area network (LAN) and smaller than a wide area network (WAN), (b) interconnects two or more LANs, and (c) usually covers an entire metropolitan area, such as a large city and its suburbs.

3.4 **Personal Digital Assistant (PDA)**. A handheld computer that serves as an organizer for personal information. It generally includes at least a name-and-address database, a to-do list, and a note taker. PDAs are pen-based and use a stylus to tap selections on menus and to enter printed characters. The unit may also include a small on-screen keyboard that is tapped with the pen. Data are synchronized between a user's PDA and desktop computer by cable or wireless transmission.

3.5 **Smart Card**. A credit card with a built-in microprocessor and memory that is used for identification or financial transactions. When inserted into a reader, the card transfers data to and from a central computer. A smart card is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times.

3.6 **Virtual Private Network**. A means by which certain authorized individuals (such as remote employees) can gain secure access to an organization's intranet by means of an extranet (a part of the internal network that is accessible via the Internet).

3.7 **Wide Area Network (WAN)**. A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and is usually spread over a larger geographic area than that of a LAN. Note 1: WANs may include physical networks, such as Integrated Services Digital Networks (ISDNs), X.25 networks, and T1 networks. Note 2: A metropolitan area network (MAN) is a WAN that serves all the users in a metropolitan area. WANs may be nationwide or worldwide.

3.8 **Wireless Application Protocol (WAP)**. A standard for providing cellular telephones, pagers, and other handheld devices with secure access to e-mail and text-based Web pages.

3.9 **Wired Equivalent Privacy (WEP)**. Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

4.0 Applicability

These guidelines are intended to be useful to all public entities that are developing their own security policies and procedures for remote access. They specifically apply to state government agencies, excluding higher educational institutions.

5.0 Responsibility

5.1 **Agency and Institutional Heads**. The highest authority within an agency or institution is responsible for the protection of information resources, including developing and implementing information security programs, including disaster recovery plans for information technology. The authority may delegate this responsibility but delegation does not remove the accountability.

5.2 **Agency Information Officer**. In most cases, the highest authority within an agency or institution delegates the general responsibility for security of the agency's information technology resources to the agency's highest-ranking information technology professional. This responsibility includes development and promulgation of agency-specific information security policies, including disaster recovery planning for information technology.

5.3 **Agency Security Officer**. In some cases, the Agency Information Officer assigns an Agency Security Officer who is responsible for preparing a disaster recovery plan for information technology. They must understand the risks posed by disruption of computer systems. They must help prepare contingencies and be ready to implement the disaster recovery plan for information technology.

6.0 Related Policies, Standards and Guidelines

6.1 NITC Security Officer Handbook (http://www.nitc.state.ne.us/standards/security/so_guide.doc)

6.2 NITC Network Security Policy (http://www.nitc.state.ne.us/standards/index.html)

6.3 NITC Incident Response and Reporting Procedures for State Government (http://www.nitc.state.ne.us/standards/index.html)

7.0 References

7.1 National Institute Standards and Technology (NIST) Special Publication, 800-46, "Security for Telecommuting and Broadband Communications". A full copy of this publication is available at: (http://csrc.nist.gov/publications/nistpubs/index.html).

APPENDIX

A. Home Computer Security Checklist

1. **Anti Virus Software --** Anti virus application is installed and is configured to:
    a. Start with the boot of the operating system.
    b. Run in the background and automatically scan all incoming files.
    c. Enable web browser protection, if available.
    d. Automatically update the virus signature database weekly.
    e. Schedule it to be run at least weekly to scan all hard drive files.
    f. Attempt to recognize unknown viruses, if available.
2. **Spyware Removal Tools**
    a. Install and run a spyware removal tool to identify and eliminate (as appropriate) spyware.
    b. On a monthly basis, update and run spyware removal tool, again eliminate discovered spyware if appropriate.
3. **Firewall**
    a. A firewall is an application that is employed to monitor and limit dangerous packets from entering a network, providing the capability to:
    b. Log all suspicious traffic (this is generally true for default installs).
    c. Examine log on a periodic basis.
    d. Block traffic to ports that support services that should not be accessible from the Internet (e.g., NetBIOS, Telnet, etc.).
    e. Automatically lock out network access to the host when network connectivity is not required (e.g., when the screensaver activates or computer is inactive for a fixed period of time).
    f. Notify the user when an application attempts to make an outbound connection.
    g. Medium to high level of security (e.g., “paranoia level”).
4. **Encryption Software**
    a. Ensure that appropriate encryption software is being used.
5. **Securing the Operating System**
    a. Secure or disable file and printer sharing.
    b. Ensure that the latest operating system patches are installed.
    c. Use a password protected screensaver to lock it during periods of inactivity.
    d. Where appropriate use a BIOS password to restrict who is able to start the system.
    e. Turn your system off when it is not being used.
6. **Securing Wireless Networks**
    a. Place wireless base station away from outside walls in order to minimize transmission of data outside of building.
    b. Use additional encryption beyond WEP (VPN, PGP, etc.).
    c. Enable 128-bit WEP encryption.
    d. Change SSID to a hard to guess password.
    e. Enable additional authentication schemes supported by your wireless base station.
    f. Disable broadcasts of SSID in the wireless base station beacon message.
    g. Disable SNMP or change the SNMP community strings to a hard-to-guess password.
    h. Install personal firewall on all wireless clients.
7. **Online Security Assessment**
    a. An online security assessment has scanned the current configuration (including the firewall).
    b. All major vulnerabilities identified by the assessment have been corrected and confirmed by a rescan.
8. **Securing Web Browsers**
    a. Browser(s) configured to limit or disable plugins.
    b. Browser(s) configured to limit ActiveX, Java, and JavaScript.

B. **Laptop Security Checklist**

The need for an explicit laptop security checklist can be illustrated by the fact that, according to Safeware Insurance in 1999, the number of laptop computers stolen outnumbered the number of desktop computers stolen by almost 12 to 1.

1. **Review Home Computer Security Checklist**
   a. Where applicable, the appropriate elements from the home computer security checklist presented previously should be applied to a laptop computer. (Not all elements from home computer security checklist may apply.)
2. **Encryption Software**
   a. Although mentioned above in the home computer security checklist, encryption is vital for protecting sensitive information on a mobile computer. Operating system features such as encrypting file system (EFS) or even discretionary access control (DAC) permissions can provide valuable security for a laptop that is stolen.
   b. Third-party software such as PGP and Norton Internet Security can provide similar levels of protection for laptop data.
3. **Physical Security**
   a. Laptops that spend a majority of their time in two or fewer places should be physically secured with a cable lock.
   b. Cable locks are widely available on the Internet and in computer retail stores.
   c. Almost all major laptop brands contain a slot to attach a lock cable.
   d. Those that do not can have a lock cable glued on.
4. **Set BIOS Password**
   a. Set BIOS password to prompt user every time laptop is powered up.
   b. Check for BIOS updates at least twice a year (or more) to “flash” BIOS.
5. **Use Non-descript carrying case**
   a. Avoid unwanted attention. A leather briefcase or obvious laptop case can attract attention in public places, especially airports, and while on planes.
   b. If traveling with confidential information, pack information or information backup in separate bag from laptop in case of theft.
6. **Identify Laptop with contact information**
   a. Many companies and individuals place decals or markings on the laptop case that are difficult to remove and if done so, indicate obvious tampering.
   b. Record serial number and other identification information about laptop twice, and keep one copy at home or in the office in case of theft. This information can be helpful to authorities searching for the laptop.
7. **Backup all personal data on a regular basis**
   a. In the event that your laptop is stolen, all of your work is essentially useless without a backup of all of your personal data.
8. **Consider purchasing advanced security features**
   a. Should your computing needs or data security warrant it, products that offer increasingly advanced security features such as biometric login, motion sensing, and “Lo-Jack” type location tracking are becoming increasingly cheaper to purchase for laptops.
   b. Software developers are responding to this demand by integrating these new technologies into common tasks of computer usage such as seamlessly logging in to the operating system.

C. **Telecommuting Security Checklist**

This checklist originally appeared in a Department of Energy publication. Not all items in the list will apply to every organization or telecommuter, but it provides a helpful starting point for an organization or individual to review the security of home computer systems. The checklist also includes considerations for organizations that have telecommuting users who regularly access the organization’s central network.

1. **User Identification and Authorization**
   a. Is the telecommuter authorized by their supervisor/manager to telecommute?

   b. Is the telecommuter authorized by the system owner to access the system(s) remotely?
   c. Does the telecommuter have a unique user ID and password for remote access and for access to sensitive applications?
2. **Access Controls**
   a. Are system access controls in place and functioning to log the identification of each remote access user, device, port, and user activity?
   b. Are system audit logs protected from unauthorized access?
   c. Are banners displayed regarding monitoring for unauthorized access and misuse?
3. **Auditing**
   a. Does the remote access system record alarms and authentication information?
   b. Does the system audit log identify date and time of access, user, origin, success or failure of access attempt?
   c. Are system audit logs retained to support reviews by computer security personnel?
   d. If dial-up access is allowed, does the system record details of access attempts?
4. **Information Availability**
   a. Are Government information assets (hardware, software, data, records) in a physically secure location and protected from theft, fire, smoke, hazardous material, etc.?
   b. Is backup media maintained, secured, and easily retrieved to support established contingency and disaster recovery plans?
   c. Is a physical inventory periodically conducted of Government information assets used for telecommuting?
   d. Can Government information assets be retrieved in the event of employee termination?
   e. Is there a process in place to ensure the most current version of anti virus software is installed on the telecommuting computer?
   f. Are Government information assets adequately secured when not in use by the telecommuter?
   g. Are user IDs and passwords protected from unauthorized use?
5. **Information Confidentiality**
   a. Is Government information protected from unauthorized disclosure (family, friends, eavesdroppers)?
   b. Is encryption used when transmitting sensitive unclassified information?
6. **Remote Access Security Administration**
   a. Is organizational, system administrator, and user responsibility for remote access security defined?
   b. Are justifications for remote access users periodically revalidated to support continued access privileges commensurate with job duties (at least annually)?
   c. Are incident reporting procedures in place to address handling of security breaches?
   d. Is regular system monitoring performed to detect unauthorized access attempts, denial of service, or other security weaknesses?
   e. Is access to network management tools restricted to authorized users?
   f. Is software used for telecommuting legally purchased, and are software-licensing agreements properly maintained?
   g. Are telecommuting equipment hard drives degaussed or overwritten to remove sensitive information in accordance with established best business practices?
7. **Architecture and Network Topology**
   a. Is the telecommuting equipment used interoperable with the computing architecture deployed at the home office?
   b. Does the network adequately separate traffic according to user communities? Does the remote access equipment and system protect the internal trusted network from the external (public) untrusted network?
   c. Are network topology maps documented and kept current?
8. **Education, Awareness, and Enforcement**

   a. Are telecommuters and their supervisors trained in the specific risks, threats, vulnerabilities, and proper use of a secure telecommuting environment?
   b. Is the telecommuter current on their computer security training?
   c. Is the telecommuter aware of the consequences for violation of Condition of Use agreements?

9. **Modem Use**
   a. Is there a single (or otherwise restricted) point of entry via modem into the internal network or server?
   b. Are all dial-up numbers protected from unauthorized disclosure?
   c. Is the telecommuter instructed to disconnect modem connectivity to the home office network or server when not in use?

NEBRASKA INFORMATION
TECHNOLOGY COMMISSION

TECHNICAL STANDARDS AND GUIDELINES

XX-XX-XX Use of Computer-based Fax Services by State Government Agencies

Category	**Groupware Architecture**
Title	**Use of Computer-based Fax Services by State Government Agencies**
Number	**03-01-03**

Applicability

☑ **State Government Agencies**

☑ All..**Guideline**

☐ Excluding: ________________.....**Not Applicable**

☐ **State Funded Entities -** All entities receiving state funding for matters covered by this document.................**Not Applicable**

☑ **Other:** Public Entities, see §4.2 ....**Guideline**

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of ____________.
Guideline - Adherence is voluntary.

Status	☐ Adopted ☑ Draft ☐ Other:________
Dates	Date: July 11, 2003 Date Adopted by NITC: Other:

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-1506(6)
http://www.nitc.state.ne.us/standards/

1.0 Technical Guideline

State agencies needing fax services based on electronic mail systems should consider utilizing the “eFax” system maintained and hosted by IMServices. Agencies are encouraged to contact IMServices for more information and a cost-benefit analysis.

State agencies needing facsimile services that do not choose to use the eFax system maintained and hosted by IMServices must contact the Division of Communications. (See 5.2 below.)

2.0 Purpose and Objectives

The purpose of this guideline is to provide state government agencies a suggested technical solution for sending and receiving electronic faxes directly from personal computers.

2.1 Background

Sending Faxes - The traditional method for sending faxes is to scan printed copy into a facsimile machine and manually entering a phone number to transmit a copy to an external fax machine. This method consumes staff time when copies must be sent to multiple destinations. Sequential transmissions to a large number of recipients can take too much time in an emergency situation.

Some agencies have contracted for mass distribution services from external companies. These services can be costly and require advance arrangements for entering recipient fax connection information.

An alternative method for faxing documents is the use of a high-capacity, state-run fax server activated directly from personal computers. The sender never leaves the workstation and can fax announcements directly from existing agency e-mail systems. The body of the e-mail can include a wide array of attachment formats.

Destination fax numbers can be stored in email address books. Group lists can be used for mass distribution. Multiple destination fax machines can be contacted at the same to reduce the total time to deliver information in an emergency situation.

For agencies with non-standard e-mail, it is possible to utilize a web site to send faxes.

Receiving Faxes - The traditional method for receiving faxes is to have incoming faxes printed at a local facsimile machine. An attendant watches for incoming faxes and manually routes the document to the intended user. Photocopies must be produced manually when the information needs to be routed to several people.

A fax server routes incoming faxes to an e-mail inbox where the information can be reviewed for distribution. This electronic image can be forwarded to multiple e-mail addresses without need from printing or photocopy services.

An added benefit of receiving electronic fax images is that the image can be copied into a document management system for processing without the need for scanning the printed faxes.

eFax - Three agencies, Information Management Services (“IMServices”), Health and Human Services (“HHS”) and Workers’ Compensation Court, identified a need for the use of a fax server. In a collaborative effort, these agencies are sharing the use of a fax server maintained and hosted by IMServices. A fax server is a computer connected to a network that uses a pooled collection of phone lines for users to send and receive faxes.

The state run electronic fax server system, called “eFax”, is available for use by other agencies within state government.

3.0 Definitions

3.1 Facsimile

A document sent over telephone lines, originally by means of a special facsimile machine which scans a document and transmits electrical signals to print a copy of the document on the other end. Facsimile services are a telecommunications service and are covered by the statutory authority of the Division of Communications.

3.2 Fax server

A computer in a network that uses a pooled collection of telephone lines for users to send and receive faxes.

3.3 eFax

A fax server maintained and hosted by IMServices for use by state government agencies that uses electronic mail for sending and receiving faxes.

4.0 Applicability

4.1 State Government Agencies

Adherence to this guideline is voluntary with regard to utilizing the eFax server. State agencies choosing to use facsimile services outside of the eFax server are advised that state statutes require the service to be purchased through the Division of Communications.

4.2 Other Entities

Other public agencies may use the eFax server, if they are connected to the State's network.

5.0 Responsibility

5.1 IMServices

The eFax server is hosted and maintained by IMServices.

Contact Information:

Kevin Keller, IMServices	or	Ron Ritchey
(402) 471-0655		(402) 471-7956
kkeller@notes.state.ne.us		Ron.Ritchey@email.state.ne.us

5.2 Division of Communications

State statutes § 81-1120.01 through § 81-1120.28 define the authority of the Division of Communications as it relates to the purchase of telecommunications services for state government agencies in Nebraska.

Contact Information:
To purchase a traditional facsimile machine, see the website indicated in 6.0. For other types of services, or to contact an individual regarding facsimile options, contact:

Bob Howard, Telecommunications Manager, Division of Communications
(402) 471-3720
bhoward@doc.state.ne.us

6.0 Related Documents

6.1 Division of Communications' List of Pre-Approved Facsimile Machines

(http://www.doc.state.ne.us/telecomm/Facsimiles.html)